RETOS Y NOVEDADES EN EL SISTEMA DE PROPIEDAD INTELECTUAL.

UNA MIRADA DESDE EL REGUMEN DE LOS DERECHOS DE AUTOR Y LAS NUEVAS TECNOLOGIAS

Compilador y Editor:

Wilson Danilo Ibarra Rosero

PÁGINA LEGAL

Título completo de la obra:

Retos y novedades en el sistema de propiedad intelectual, una mirada desde el régimen de los derechos de autor y las nuevas tecnologías

Compilador y editor académico:
Wilson Danilo Ibarra Rosero
C.C. 1085263276
daniloibarrarosero@gmail.com

Primera edición
Pasto, Colombia, agosto de 2025

© Todos los derechos reservados

Ninguna parte de esta publicación, incluida la totalidad o parte de sus textos, imágenes o ilustraciones, puede ser reproducida, almacenada o transmitida en ninguna forma ni por ningún medio —electrónico, mecánico, fotocopia, grabación u otros— sin autorización escrita del compilador/editor.

Esta obra es de carácter académico y colectivo**,** publicada con fines investigativos, pedagógicos y de divulgación científica, sin fines comerciales. El contenido es responsabilidad exclusiva de los autores, quienes ceden los derechos patrimoniales a favor del compilador/editor para efectos de difusión, registro y distribución digital no lucrativa.

Créditos editoriales:
Corrección de estilo: **Wilson Danilo Ibarra Rosero**
Diseño editorial: **Wilson Danilo Ibarra Rosero**
Revisión académica: **Wilson Danilo Ibarra Rosero**

ISBN: *En trámite ante la Agencia ISBN de la Cámara Colombiana del Libro*

Formato de publicación: Digital (PDF y Word)
Idioma: Español
Tiraje: Edición única – Primera edición digital
Fecha de publicación prevista: 1 de agosto de 2025

Lugar de publicación:
Pasto, Nariño – Colombia

Tabla de contenido

CAPITULO 1..... 5

IA, PRIVACIDAD Y Ciberseguridad: CREANDO MARCOS LEGALES PARA LA REVOLUCION DIGITAL..... 5

RESUMEN..... 6

INTRODUCCIÓN 7

ANTECEDENTES..... 9

METODOLOGIA 13

DESARROLLO DE LA METODOLOGIA 13

ANALISIS DE CASOS RELEVANTES Y JURISPRUDENCIA. 18

EN EL CONTEXTO COLOMBIANO.....18

EN EL CONTEXTO INERNACIONAL.....22

CONCLUSIONES.....38

CAPÍTULO 2 39

LOS DERECHOS DE AUTOR EN LOS SISTEMAS MUSICALES DEL SIGLO XXI, UNA ALTERNATIVA DESDE EL CONTEXTO LOCAL E INTERNACIONAL COLOMBIANO. 39

RESUMEN.....40

DELIMITACION DEL PROBLEMA.....41

ARGUMENTACION. 47

NORMAS.....48

EN MATERIA DE PROPIEDAD INDUSTRIAL.....51

CONCLUSIONES.....53

CAPITULO 3 54

DESAFIANDO LA ERA DIGITAL - UNA VISION HACIA LOS CONTRATOS DE ADHESION ELECTRONICA REDES SOCIALES. 54

RESUMEN.....55

INTRODUCCION.....56

PLANTEAMIENTO DEL PROBLEMA.....57

HIPOTESIS. 58

JUSTIFICACION.....58

MARCO DE REFERENCIA.....59

PROTECCION DE LA INTIMIDAD Y LA DIGNIDAD EN CONTRATOS ELECTRONICOS EN EL CONTEXTO COLOMBIANO.....60

METODOLOGIA. 60
EL USO DE DATOS PERSONALES EN LAS REDES DE META. 61
LA CESION DE DERECHOS Y LA PROPIEDAD INTELECTUAL SOBRE LAS PUBLICACIONES....68
LOS MECANISMOS DE PROTECCION EXISTENTES....74
¿SE VULNERAN LOS DERECHOS DE AUTOR AL ACEPTAR LAS POLITICAS DE PRIVACIDAD DE META? 75
ARGUMENTOS A FAVOR DE LA VULNERACION DE DERECHOS DE AUTOR....76
ARGUMENTOS EN CONTRA DE LA VULNERACION DE DERECHOS DE AUTOR....76
QUE PASA CON EL DERECHO DE IMAGEN EN LAS PLATAFORMAS DIGITALES. 75
MARCO LEGAL Y JURISPRUDENCIA....78
RECOMENDACIONES Y FUTURO DEL DERECHO DE IMAGEN. 78
REFERENCIAS....79

CAPITULO 1.

IA, PRIVACIDAD Y Ciberseguridad: CREANDO MARCOS LEGALES PARA LA REVOLUCION DIGITAL.

Autores:

David Alexander Bravo Moncayo
Santiago Benavides Ortega
Samuel Felipe Guerrero Almeida
Wilson Danilo Ibarra Rosero

RESUMEN

La inteligencia artificial (IA) ha surgido como una herramienta transformadora en múltiples sectores, incluido el derecho informático, la de la IA para automatizar procesos, analizar datos, elegir la mejor decisión en base a algoritmos ha presentado retos y oportunidades significativas. A medida que la IA abarca áreas como la ciberseguridad, la privacidad y la administración de justicia, se vuelve menester examinar las implicaciones legales que su uso conlleva.

El presente documento explora las relaciones entre la IA, la ciberseguridad y su conexión directa con los derechos fundamentales enfocado al derecho a la privacidad y a la intimidad. En el contexto actual los datos personales se han convertido en un objeto indispensable para el desarrollo de nuevas tecnologías, la evolución de la IA ha significado un desafío para la protección de la privacidad de las personas, ya que este puede ser usada como una herramienta de amparo para bancos de datos y su mal uso puede representar una amenaza real. El presente análisis aborda el estudio de algunas de las más relevantes normas internacionales como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, hasta casos emblemáticos que han sentado precedentes en la jurisprudencia global.

INTRODUCCIÓN

La inteligencia artificial (IA) ha emergido como una tecnología disruptiva que está transformando múltiples sectores, incluyendo el derecho informático. La IA se refiere a sistemas informáticos que pueden realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de voz, la toma de decisiones y la traducción de idiomas. En el ámbito del derecho informático, la IA está siendo utilizada para automatizar procesos legales, mejorar la ciberseguridad, y gestionar grandes volúmenes de datos. Sin embargo, su adopción también plantea desafíos significativos en términos de privacidad, seguridad, y regulación legal, que requieren un análisis profundo y especializado.

En la era digital, la seguridad informática se ha convertido en una preocupación central para individuos, empresas y gobiernos. Con el creciente uso de la IA, la cantidad de datos sensibles que se generan y procesan ha aumentado exponencialmente, lo que amplía la superficie de ataque para posibles ciber amenazas. La seguridad informática, por lo tanto, no solo se centra en proteger la confidencialidad, integridad y disponibilidad de la información, sino también en asegurar que las tecnologías emergentes, como la IA, no se utilicen de manera maliciosa o negligente. Este aspecto es crucial para el desarrollo de un marco legal que proteja a los usuarios y garantice la confianza en los sistemas basados en IA.

La privacidad y la intimidad son derechos fundamentales que se ven especialmente afectados en el contexto de la tecnología digital y la IA. La recopilación masiva de datos personales por parte de sistemas de IA plantea preocupaciones sobre el control que los individuos tienen sobre su información personal y cómo esta puede ser utilizada sin su consentimiento explícito. La relevancia de la privacidad en la era digital se ha intensificado, dado que la información personal es ahora un recurso valioso que puede ser explotado por empresas y gobiernos, lo que hace necesario un análisis jurídico que evalúe las protecciones existentes y sugiera nuevas medidas para salvaguardar estos derechos.

El presente artículo tiene como objetivo analizar de manera exhaustiva las implicaciones jurídicas de la inteligencia artificial en el ámbito del derecho informático, la seguridad

informática y la intimidad. Se propone identificar los desafíos legales que plantea la implementación de IA en estos campos, evaluar la eficacia de las normativas actuales, y proponer soluciones que mejoren la protección de los derechos fundamentales. La relevancia de este análisis radica en la necesidad urgente de adaptar las leyes y regulaciones a las realidades tecnológicas emergentes, asegurando que la innovación tecnológica no comprometa los principios básicos de justicia, privacidad y seguridad. La implementación de la IA en diversas aplicaciones tecnológicas ha generado una serie de controversias y problemas que requieren una atención jurídica especializada. Entre los problemas más destacados se encuentran la falta de transparencia en los algoritmos de IA, la posible discriminación algorítmica, la vulnerabilidad a ciberataques, y las dificultades para atribuir responsabilidad legal en caso de fallos o daños causados por sistemas de IA. Estas controversias reflejan la complejidad de regular una tecnología en rápida evolución y subrayan la importancia de desarrollar un marco legal que sea flexible y adaptativo, capaz de abordar los desafíos actuales y futuros de la IA.

La rápida evolución de la inteligencia artificial ha puesto de manifiesto la necesidad urgente de un marco regulatorio robusto y adaptativo que pueda abordar los desafíos únicos que esta tecnología presenta. A medida que la IA se integra en diversas aplicaciones críticas, desde la salud hasta la seguridad nacional, es esencial que las leyes y regulaciones evolucionen para garantizar que la IA se utilice de manera segura y ética. Este marco regulatorio debe ser lo suficientemente flexible como para adaptarse a los rápidos avances tecnológicos, mientras se mantiene firme en la protección de los derechos fundamentales, como la privacidad y la seguridad. La ausencia de una regulación adecuada podría dar lugar a abusos de poder, discriminación y riesgos significativos para la sociedad.

El análisis presentado en este artículo se basa en una metodología jurídica cualitativa que combina el estudio de la doctrina, la jurisprudencia y la legislación vigente en torno a la inteligencia artificial, el derecho informático, la seguridad informática y la intimidad. Se ha realizado un estudio de tipo comparativo entre diferentes jurisdicciones para evaluar cómo las diversas normativas internacionales abordan los desafíos que presenta la IA. Además, se han utilizado casos emblemáticos en derecho y tecnología para proporcionar una visión integral de las implicaciones legales de la IA. Este enfoque permite una comprensión

profunda y crítica de los temas tratados, ofreciendo propuestas para mejorar la regulación en estos ámbitos. Lo que se busca principalmente con el desarrollo de estas técnicas de investigación presentes el escrito es presentar de una forma más clara y precisa el gran alcance que tiene hoy día el uso generalizado de las distintas inteligencias artificiales en la vida cotidiana de las personas, uso mimo que al tener un desarrollo tan acelerado permite a las personas cada vez con una mayor facilidad, encontrar puertas legales que dan pié al desarrollo de riesgo dentro del ámbito social para quienes se encuentran expuestos a estas tecnologías.

Este artículo contribuye a la literatura existente en varios frentes. En primer lugar, ofrece un análisis exhaustivo de las implicaciones jurídicas de la inteligencia artificial en el derecho informático, un área que ha sido relativamente poco explorada en la doctrina jurídica. Además, el artículo aborda la seguridad informática y la privacidad desde una perspectiva jurídica, ofreciendo una visión crítica de las normativas actuales y proponiendo mejoras basadas en un análisis comparativo de diferentes marcos regulatorios. Al hacerlo, el artículo no solo enriquece el debate académico, sino que también proporciona a los legisladores y profesionales del derecho herramientas útiles para abordar los desafíos que plantea la IA. Este estudio, aunque exhaustivo en su análisis, enfrenta ciertas limitaciones inherentes. En primer lugar, la naturaleza dinámica de la tecnología de inteligencia artificial significa que las normativas y casos de estudio pueden cambiar rápidamente, lo que podría limitar la aplicabilidad a largo plazo de algunas de las conclusiones presentadas. Además, aunque se ha realizado un análisis comparativo de diferentes jurisdicciones, el estudio se centra principalmente en el marco legal colombiano, lo que puede no ser directamente aplicable en otros contextos legales. Sin embargo, estas limitaciones se abordan mediante una discusión detallada sobre cómo las propuestas regulatorias pueden adaptarse y evolucionar en respuesta a los cambios tecnológicos.

ANTECEDENTES

La inteligencia artificial (IA) se refiere a la simulación de procesos de inteligencia humana por parte de sistemas informáticos. Estos procesos incluyen el aprendizaje, el razonamiento y la autocorrección. La IA ha evolucionado significativamente desde su concepción en la

década de 1950, pasando de ser una mera idea especulativa a convertirse en una realidad tangible con aplicaciones prácticas en diversos campos, incluyendo la medicina, la economía, la defensa y, por supuesto, el derecho. En términos generales, la IA se puede clasificar en dos categorías: IA débil, que está diseñada para realizar tareas específicas, y IA fuerte, que es hipotética y tendría la capacidad de realizar cualquier tarea cognitiva que un ser humano pueda hacer. Esta evolución plantea importantes desafíos legales, especialmente en lo que respecta a la responsabilidad, la privacidad y la ética.

El derecho informático es una rama del derecho que se ocupa de los problemas legales relacionados con el uso de las tecnologías de la información y la comunicación (TIC). Este campo abarca una amplia gama de temas, incluyendo la protección de datos, la ciberseguridad, los contratos electrónicos, los delitos informáticos y la propiedad intelectual. A medida que la tecnología evoluciona, también lo hacen los desafíos legales que surgen de su uso. Por ejemplo, la implementación de la IA en sistemas informáticos plantea preguntas sobre la responsabilidad y la regulación, dado que los sistemas de IA pueden tomar decisiones autónomas que afectan a los derechos de los individuos. El derecho informático, por lo tanto, juega un papel crucial en la creación de un marco legal que aborde estos nuevos desafíos los cuales han ganado una relevancia tan alta dentro de los marcos jurídicos de los estados ocupando así los primeros puestos de preocupación cuando se refiere a la materia normativa.

La seguridad informática se refiere a las prácticas y tecnologías utilizadas para proteger los sistemas informáticos y la información que contienen contra accesos no autorizados, daños o interferencias. Los principios fundamentales de la seguridad informática incluyen la confidencialidad, la integridad y la disponibilidad de la información. Sin embargo, la creciente sofisticación de las amenazas cibernéticas y el uso de IA en la seguridad informática han introducido nuevos desafíos. Por ejemplo, la IA puede ser utilizada tanto para mejorar la seguridad mediante la detección proactiva de amenazas, como para perpetrar ataques más sofisticados y difíciles de detectar. Este dualismo plantea preguntas sobre cómo regular el uso de la IA en la seguridad informática y cómo garantizar que las tecnologías se utilicen de manera responsable.

La intimidad y la privacidad son conceptos interrelacionados pero distintos, que se refieren a los derechos de los individuos a mantener su vida personal y su información libre de intrusiones no deseadas.

Históricamente, el derecho a la privacidad ha sido reconocido como un derecho humano fundamental en numerosas jurisdicciones el cual ha logrado tener índices de protección con alto grado de efectividad, pero su definición y alcance han evolucionado con el tiempo, especialmente en respuesta a los avances tecnológicos. En la era digital, la privacidad se ha convertido en un tema de gran preocupación debido a la capacidad de las tecnologías, incluyendo la IA, para recopilar, procesar y analizar grandes volúmenes de datos personales. Esta evolución histórica ha llevado a la creación de nuevas leyes y regulaciones diseñadas para proteger la privacidad en el entorno digital, pero también ha generado debates sobre la suficiencia y la eficacia de estas medidas.

La regulación de la inteligencia artificial varía significativamente entre diferentes jurisdicciones, reflejando diferentes enfoques hacia la innovación tecnológica y la protección de los derechos fundamentales. Por ejemplo, en la Unión Europea, la regulación de la IA está enmarcada en un enfoque de derechos fundamentales, como lo ejemplifica la propuesta de la Ley de IA, que establece estrictos requisitos para la transparencia, la responsabilidad y la ética en el uso de la IA. En contraste, en los Estados Unidos, la regulación tiende a ser más permisiva, centrada en fomentar la innovación mientras se aborda la seguridad y la privacidad a través de normas sectoriales. Este análisis comparativo resalta las diferencias en cómo los países abordan la regulación de la IA y proporciona un contexto para entender las implicaciones legales de la IA en Colombia y otras jurisdicciones.

La protección de la seguridad informática y la privacidad ha sido objeto de regulaciones a nivel internacional, que buscan establecer estándares comunes para la protección de los datos y la información personal. Entre las normativas más destacadas se encuentra el Reglamento General de Protección de Datos (GDPR)[1] de la Unión Europea, que establece estrictas directrices sobre cómo deben manejarse los datos personales, incluyendo la exigencia de consentimiento explícito, el derecho al olvido y la obligación de notificar violaciones de

[1] GDPR: reglamento de la Unión Europea que establece normas para la protección de datos electrónicos de empresas y particulares.

seguridad. Otras normativas, como La Ley de Privacidad del Consumidor de California (CCPA)[2] en los Estados Unidos, también han establecido precedentes importantes en la protección de la privacidad. Estas normativas internacionales proporcionan un marco que no solo protege a los ciudadanos, sino que también impone obligaciones a las empresas y organizaciones que manejan datos, creando un entorno más seguro y confiable para la gestión de la información en la era digital. La intersección entre la inteligencia artificial y el derecho informático es un área de creciente interés, dado que la IA está profundamente integrada en muchos aspectos de las tecnologías de la información. Esta relación plantea preguntas fundamentales sobre la regulación de los algoritmos, la protección de la propiedad intelectual y la atribución de responsabilidad cuando un sistema de IA toma decisiones autónomas que afectan a terceros. Por ejemplo, en el contexto de la ciberseguridad, los sistemas de IA pueden ser utilizados tanto para defender como para atacar infraestructuras críticas, lo que plantea la necesidad de establecer marcos legales claros que regulen su uso. El uso de la inteligencia artificial en la seguridad informática no solo plantea desafíos técnicos y legales, sino también éticos. Los sistemas de IA pueden tomar decisiones que afecten significativamente la vida de las personas, como determinar el acceso a servicios, detectar fraudes o incluso predecir comportamientos. Estas decisiones, si no están bien reguladas, pueden llevar a la discriminación, la invasión de la privacidad o la violación de derechos fundamentales.

La protección de los datos personales es uno de los desafíos más críticos en la era de la inteligencia artificial. Los sistemas de IA dependen de grandes volúmenes de datos para funcionar eficazmente, lo que incluye datos personales sensibles. Esto ha llevado a un aumento de las preocupaciones sobre la privacidad y la seguridad de los datos. La recopilación, almacenamiento y procesamiento de datos personales por parte de sistemas de IA deben cumplir con las normativas legales vigentes, como el GDPR, que establece estrictos requisitos para la protección de los datos, además de que representa dos enfoques de alcance internacional como lo son el enfoque de la denominada sustancia legal con el cual se pretende la creación de un marco sólido para la protección de datos y el enfoque de la accesibilidad por el cual distintas jurisdicciones podrían adoptar sus medidas (Schwartz, 2022). entendiendo así que es fundamental que se implementen medidas técnicas y organizativas

[2] Ley del estado de California que otorga a sus residentes derechos sobre sus datos y obligaciones para las empresas que se dedican a almacenarlos.

adecuadas para proteger los datos contra accesos no autorizados, pérdidas o daños. La implementación de IA también plantea la cuestión del consentimiento informado, ya que los individuos deben tener un control real sobre cómo se utilizan sus datos. Por lo tanto, la protección de datos en la era de la IA no es solo una cuestión de cumplimiento legal, sino también de confianza y responsabilidad social.

METODOLOGIA

La metodología adoptada en este artículo combina un enfoque cualitativo riguroso con técnicas avanzadas de análisis de datos para explorar las implicaciones jurídicas de la inteligencia artificial en el derecho informático, la seguridad informática y la privacidad. A través del análisis doctrinal, la revisión de la jurisprudencia, las entrevistas con expertos y el uso de herramientas tecnológicas, se logró un análisis profundo y bien fundamentado el cual permite entender un poco más todo el mundo de la inteligencia artificial y como esta ha adentrando en la normalidad del día a día.

DESARROLLO DE LA METODOLOGIA

Este artículo se centra en examinar de manera exhaustiva las implicaciones jurídicas de la inteligencia artificial en el derecho informático, la seguridad informática y la privacidad. Esta sección aborda la intersección de estas áreas, explorando cómo la IA está transformando el panorama legal y los desafíos que plantea para la regulación. Se analiza cómo la IA puede ser tanto una herramienta poderosa para mejorar la seguridad y la eficiencia en la gestión de la información como una fuente de riesgos significativos si no se regula adecuadamente. A través de un enfoque multidisciplinario, se exploran los impactos legales de la IA desde diversas perspectivas, incluyendo la responsabilidad, la ética, la protección de datos y la ciberseguridad.

La inteligencia artificial ha comenzado a integrarse en el derecho informático de maneras que desafían las nociones tradicionales de regulación y cumplimiento legal. Por ejemplo, los sistemas de IA son utilizados para automatizar procesos legales, como la revisión de contratos y la detección de fraudes, lo que plantea preguntas sobre la fiabilidad y la

imparcialidad de estas tecnologías. Además, la IA está redefiniendo conceptos clave del derecho informático, como la privacidad y la seguridad, al permitir la recopilación y análisis de grandes volúmenes de datos. Este análisis destaca la necesidad de un marco regulatorio que no sólo proteja los derechos de los individuos, sino que también fomente la innovación tecnológica dentro de límites éticos y legales bien definidos.

La seguridad informática se ha visto profundamente afectada por el desarrollo y la implementación de la inteligencia artificial. Los sistemas de IA pueden ser utilizados tanto para mejorar la seguridad, mediante la detección proactiva de ciberamenazas y la respuesta automática a incidentes, como para perpetrar ataques más sofisticados y difíciles de detectar. Por ejemplo, la IA permite la creación de malware avanzado que puede evadir las defensas tradicionales y adaptarse a las medidas de seguridad en tiempo real. Esta dualidad de la IA en la seguridad informática plantea desafíos significativos para los reguladores, quienes deben equilibrar la promoción de la innovación con la necesidad de proteger las infraestructuras críticas y los datos personales. Además, la IA también plantea preguntas sobre la responsabilidad legal en caso de fallos en la seguridad o ciberataques exitosos, especialmente cuando estos son facilitados por tecnologías autónomas.

La inteligencia artificial ha cambiado radicalmente el modo en que se maneja la privacidad en el entorno digital. Los sistemas de IA tienen la capacidad de analizar grandes volúmenes de datos personales en cuestión de segundos, lo que permite la creación de perfiles detallados de individuos y grupos. Esto plantea serias preocupaciones sobre la privacidad, especialmente en lo que respecta al consentimiento informado y la capacidad de los usuarios para controlar cómo se utilizan sus datos. Además, la IA puede ser utilizada para monitorear y analizar el comportamiento de los usuarios en línea, lo que lleva a la erosión de la privacidad y la posible explotación de la información personal con fines comerciales o gubernamentales. Desde un punto de vista jurídico, es fundamental desarrollar y fortalecer las normativas que protejan la privacidad en la era de la IA, asegurando que los derechos fundamentales de los individuos sean respetados y que existan mecanismos efectivos para responsabilizar a las entidades que manejan datos personales.

La protección de datos personales en el contexto de la inteligencia artificial es una de las áreas más críticas del derecho informático. Los sistemas de IA dependen en gran medida de

grandes volúmenes de datos para su entrenamiento y operación, lo que plantea serias preocupaciones sobre cómo se recopilan, almacenan y utilizan estos datos. La implementación de IA en la toma de decisiones automatizadas puede llevar a la exposición de información sensible, lo que subraya la necesidad de marcos regulatorios sólidos que protejan la privacidad de los individuos. En este sentido, legislaciones como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea sirven como referencia global, estableciendo estándares rigurosos para la gestión de datos personales. Sin embargo, en muchas jurisdicciones, incluidas algunas en América Latina, aún existen vacíos legales que deben ser abordados para asegurar que los derechos de privacidad sean adecuadamente protegidos frente a la creciente influencia de la IA.

La seguridad informática es otro aspecto fundamental donde la inteligencia artificial juega un rol cada vez más importante. Los sistemas de IA pueden ser tanto una herramienta poderosa para mejorar la ciberseguridad, al detectar y responder a amenazas en tiempo real, como un vector de ataque si son mal utilizados. Esto genera preguntas complejas sobre la responsabilidad legal en caso de fallos de seguridad. Por ejemplo, si un sistema de IA falla en prevenir un ciberataque, o si es utilizado para perpetrar uno, ¿quién debe ser considerado responsable? Este es un desafío que la legislación actual aún no aborda de manera clara, lo que crea incertidumbre tanto para los desarrolladores de tecnología como para los usuarios. La creación de un marco legal que defina claramente las responsabilidades en materia de seguridad informática es crucial para asegurar que la IA se utilice de manera segura y ética.

La implementación de la inteligencia artificial en diversas áreas, especialmente en la vigilancia y el monitoreo, ha planteado serias preocupaciones sobre la intimidad y los derechos fundamentales. La capacidad de la IA para analizar grandes cantidades de datos y reconocer patrones puede resultar en la invasión de la privacidad y en la erosión de la intimidad de los individuos. Esto es especialmente preocupante en contextos donde se utiliza la IA para la vigilancia masiva o el reconocimiento facial, tecnologías que pueden ser empleadas por gobiernos y empresas para monitorear a las personas sin su consentimiento. Desde un punto de vista jurídico, es esencial que la regulación de la IA se alinee con los principios de protección de los derechos humanos, garantizando que su uso no socave la dignidad ni la libertad de los individuos.

A medida que la inteligencia artificial continúa avanzando, varios países han comenzado a desarrollar proyectos de ley para regular su uso. Estos proyectos de ley varían en su enfoque, desde la protección de datos y la privacidad hasta la responsabilidad en caso de daños causados por sistemas de IA. Un ejemplo destacado es la propuesta de la Ley de IA de la Unión Europea, que busca establecer un marco legal integral para regular el desarrollo y la implementación de IA en todos los sectores. Esta ley propone clasificar los sistemas de IA según su nivel de riesgo y establecer requisitos específicos para cada categoría, desde sistemas de alto riesgo, como los utilizados en la atención médica, hasta aquellos de bajo riesgo. La evolución de estos proyectos de ley refleja un esfuerzo por equilibrar la innovación tecnológica con la necesidad de proteger los derechos fundamentales y la seguridad pública.

La regulación internacional de la inteligencia artificial tiene un impacto significativo en la legislación local, especialmente en países que buscan integrarse en la economía global y adoptar las mejores prácticas internacionales. Las normativas establecidas por organismos como la Unión Europea o la OCDE a menudo sirven como modelos para la legislación en otras jurisdicciones. Sin embargo, la adopción de estas normativas puede enfrentar desafíos debido a diferencias culturales, económicas y sociales. Por ejemplo, la implementación de regulaciones estrictas sobre IA en países en desarrollo puede ser más difícil debido a limitaciones en infraestructura y recursos. Es crucial que las regulaciones internacionales sean adaptadas cuidadosamente al contexto local para asegurar que sean efectivas y justas. Además, la cooperación internacional es esencial para enfrentar los desafíos globales que plantea la IA, como la ciberseguridad y la protección de la privacidad, que trascienden las fronteras nacionales.

La intersección entre ética y derecho en el contexto de la inteligencia artificial es un área de creciente interés y preocupación. A medida que los sistemas de IA se vuelven más autónomos y capaces de tomar decisiones complejas, surgen preguntas sobre los principios éticos que deben guiar su desarrollo y uso. Desde una perspectiva jurídica, es fundamental que la regulación de la IA incorpore consideraciones éticas, asegurando que las tecnologías se utilicen de manera que respeten los derechos humanos y promuevan el bienestar social. Por ejemplo, es necesario establecer límites claros para evitar la discriminación algorítmica y garantizar la equidad en la toma de decisiones automatizadas. Además, la transparencia en

los procesos de toma de decisiones de la IA es crucial para mantener la confianza pública y garantizar que las tecnologías se utilicen de manera responsable.

Los derechos de los usuarios en el contexto de la inteligencia artificial son un aspecto central que debe ser protegido por la legislación. A medida que la IA se integra cada vez más en la vida cotidiana, es fundamental que los usuarios tengan control sobre cómo se utilizan sus datos y que se les garantice la posibilidad de recurrir en caso de decisiones automatizadas que les afecten negativamente. Esto incluye el derecho a la explicación, es decir, el derecho a entender cómo y por qué un sistema de IA tomó una determinada decisión, y el derecho a la corrección o rectificación en caso de errores. Además, es esencial que los usuarios tengan acceso a mecanismos efectivos de queja y reparación en caso de que sus derechos sean violados por sistemas de IA. Proteger estos derechos no solo es una cuestión de justicia, sino también de mantener la confianza pública en el uso de tecnologías avanzadas.

La protección de la privacidad en la era de la inteligencia artificial requiere una revisión y fortalecimiento de las normativas legales existentes. Dado que los sistemas de IA dependen en gran medida de la recopilación y análisis de datos personales, es crucial que las leyes de protección de datos se adapten para abordar los nuevos riesgos que plantea esta tecnología. Esto incluye no sólo la protección contra la recopilación no autorizada de datos, sino también la regulación del uso de los datos recopilados para evitar su explotación con fines comerciales o de vigilancia. Además, es fundamental que las leyes garanticen la seguridad de los datos almacenados y que los usuarios tengan control sobre quién puede acceder a su información. La protección legal de la privacidad en el contexto de la IA no solo es una cuestión de derechos individuales, sino también de preservar la dignidad humana en un mundo cada vez más digitalizado.

El uso de inteligencia artificial en la seguridad informática plantea tanto oportunidades como riesgos en la lucha contra el cibercrimen. Por un lado, la IA puede ser utilizada para detectar y prevenir ataques cibernéticos de manera más eficiente que las tecnologías tradicionales, al identificar patrones de comportamiento sospechosos y responder a amenazas en tiempo real. Por otro lado, la IA también puede ser utilizada por los ciberdelincuentes para desarrollar ataques más sofisticados y difíciles de detectar, como el uso de malware inteligente que puede adaptarse a las defensas de las víctimas.

ANALISIS DE CASOS RELEVANTES Y JURISPRUDENCIA.

El análisis de casos relevantes y la jurisprudencia existente proporciona una base importante para entender cómo se están abordando los desafíos legales que plantea la inteligencia artificial. En varios casos, los tribunales han tenido que enfrentar cuestiones complejas relacionadas con la responsabilidad por decisiones tomadas por sistemas de IA, la protección de la privacidad y la seguridad de los datos. Entre ellos encontramos:

EN EL CONTEXTO COLOMBIANO.

El marco legal colombiano ha comenzado a adaptarse a los desafíos que plantea la inteligencia artificial, particularmente en los ámbitos del derecho informático y la seguridad informática. La Ley 1581 de 2012[3], conocida como la Ley de Protección de Datos Personales, establece los principios para la recolección, manejo y protección de los datos personales en Colombia. Sin embargo, esta ley, al igual que muchas otras normativas, no aborda de manera específica las particularidades de la IA, lo que deja un vacío en la regulación de aspectos clave como la transparencia, la responsabilidad y la ética en el uso de la IA. Además, el El Decreto 1074 de 2015[4] regula aspectos relacionados con la protección de los derechos de los titulares de datos, pero nuevamente, no aborda las complejidades introducidas por la inteligencia artificial. La necesidad de actualizar y expandir el marco legal colombiano es evidente, especialmente para garantizar que las innovaciones tecnológicas se integren de manera segura y responsable en la sociedad. La relación entre la inteligencia artificial y la privacidad ha sido objeto de intensos debates académicos, con opiniones divididas sobre cómo equilibrar la innovación tecnológica con la protección de los derechos fundamentales. Algunos académicos argumentan que la IA, por su capacidad de procesar grandes volúmenes de datos, representa una amenaza significativa para la privacidad, especialmente cuando se utiliza en combinación con tecnologías como la vigilancia masiva o el reconocimiento facial. Otros, sin embargo, sostienen que la IA puede ser una herramienta poderosa para mejorar la

[3] Ley que regula la protección de datos personales en Colombia, establece directrices y principios para la protección y tratamiento de los mismos

[4] Orientado a la protección de datos en distintos sectores, contiene distintas disposiciones que regulan la Ley 1581 de 2012.

privacidad, por ejemplo, mediante la detección y prevención de violaciones de datos. Estos debates subrayan la complejidad del tema y la necesidad de una regulación cuidadosa que equilibre estos intereses contrapuestos. Es crucial que el marco legal no sólo proteja la privacidad, sino que también permita a la IA alcanzar su potencial para el bien público, dentro de límites éticos bien definidos.

La implementación de la inteligencia artificial presenta tanto riesgos como beneficios que deben ser cuidadosamente considerados desde una perspectiva jurídica. Entre los riesgos más destacados se encuentran la posibilidad de discriminación algorítmica, la falta de transparencia en los procesos de toma de decisiones, y la dificultad para atribuir responsabilidad legal en caso de errores. Por otro lado, la IA también ofrece numerosos beneficios, como la capacidad de mejorar la eficiencia en la prestación de servicios legales, la detección de fraudes, y la protección contra ciber amenazas. El futuro de la investigación en inteligencia artificial y derecho se perfila como un campo dinámico y en constante evolución. Algunas de las áreas clave que requerirán un mayor enfoque incluyen el desarrollo de marcos regulatorios globales que puedan ser adaptados a las realidades locales, la creación de mecanismos efectivos de supervisión y control, y la integración de principios éticos en el diseño y la implementación de sistemas de IA.

SENTENCIA T 323 DE 2024, CORTE CONSTITUCIONAL, SALA SEGUNDA DE REVISIÓN.

Sentencia T-323 de 2024 de la sala segunda de revisión de la Corte Constitucional que hace referencia uso de herramientas de inteligencia artificial en procesos judiciales de tutela la cual representa para el país un avance significativo para la regulación del uso de las inteligencias artificiales dentro de la actividad de impartir justicia dentro del estado, en la misma la corte constitucional se da a la tarea de revisar el buen uso del motor de inteligencia artificial CHAT GPT 3.5 dentro de la construcción de una respuesta legal para una tutela presentada en el año 2022 con la cual se buscaba garantizar el derecho a la salud de un menor de edad diagnosticado con trastorno del espectro autista por medio de la exoneración del pago de cuotas medias copagos a la EPS así como también la obligación a la misma a dar

garantías al menor sobre el transporte al lugar de las terapias que son fundamentales para el tratamiento médico que el último necesita.

Más allá de evaluar lo referido a los hechos presentados en la tutela, la corte se vio obligada a revisar si el uso de CHAT GPT 3.5 por parte del juez de segunda instancia encargado de proferir el fallo no representaba una vulneración a una amalgama de derechos fundamentales como lo es el derecho al derecho al debido proceso de los accionantes que se pudieron haber visto violentados ya que el hacer uso de las herramientas de inteligencia artificial representa siempre estar expuestos a un grado de fallo y decisiones infundadas mucho más elevado que cuando se hace uso netamente del desarrollo de ideas humanas.

Los motivos que llevaron a la corte a iniciar dicha revisión se resumen en, poder determinar si realmente fue el juez quien finalmente desarrolló el fallo en su totalidad recibiendo el apoyo de la inteligencia artificial o si fue esta última haciendo uso de arbitrariedades la que creó el fallo que dio solución a la acción presentada lo cual representaría no solo una negligencia por parte del ente judicial sino también una vulneración grave a los derechos al debido proceso de los accionantes y también a los principios mismos del sistema de justicia del estado.

La evaluación por parte del órgano fue entonces un avance gigante en la rama judicial, ya que nos damos cuenta de que los órganos de la misma están ya pasando la lupa al actuar de sus funcionarios quienes tienen sobre sus hombros la responsabilidad de llevar la justicia a todos los rincones del país.

Sobre el fallo al que llegó la corte, se determinó que el operario de la justicia utilizó la inteligencia artificial, no para crear el fallo sino más bien la usó solo en el momento en el que el mismo ya estaba terminado, esto después de haber promovido un fallo basado siempre en preceptos legales, métodos de toma de decisiones netamente humanos, así como la protección de la integridad del menor involucrado. En este caso el juez dio uso a ChatGPT como medio para realizar preguntas de la acción, pero solo como medio ilustrativo ya que en ningún momento el motor de búsqueda de la inteligencia artificial recibió datos personales del menor

involucrado ni tampoco información sensible del asunto que hubiera podido configurar una violación incluso a los derechos de intimidad y el principio de privacidad.

Como un precedente legal la sentencia de la corte representa un hito dentro del desarrollo para la regulación del uso de inteligencias artificiales en Colombia, esto basado en que la misma determina parámetros que si bien, no prohíben de manera tajante que las inteligencias artificiales sean usadas dentro de la función de impartir justicia dentro del estado, si determina que éstas deberán servir solo como un herramienta de apoyo para los operarios de la justicia, pero jamás como un reemplazo para los mismos, la corte determina que en la toma de decisiones siempre deberá primar el uso de la razón humana la cual es el pilar fundamental dentro del sistema de justicia colombiano y no deberá ser reemplazada bajo ningún caso, ya que de ser así, se estaría siempre ante el riesgo de que las decisiones judiciales que emita una herramienta de inteligencia artificial pueda estar sujeta al uso de prejuicios o arbitrariedades los cuales para un sistema digital son casi imposibles de eludir.

Lo presentado de dentro de la sentencia podría también analizarse dentro del campo del impacto para el sector legal en Colombia, ya que el uso de estas inteligencias podría representar una vía efectiva de descongestión judicial el cual es hoy uno de los problemas más graves que enfrenta la ama además de que podría ser también la manera más efectiva de garantizar el derecho del acceso a la justicia (Lizcano Luna, 2020).

La corte además realizó un llamado a todos los operarios de la justicia para estos tengan presente el deber de llevar a cabo procesos con el más alto grado de ética en los casos en los que se vea la necesidad de hacer uso de estas herramientas, esto con miras de dar garantías totales a la protección de los derechos fundamentales de las personas que ven en el sistema de justicia un amparo en situaciones de vulnerabilidad. Como si fuera poco, resulta interesante evaluar cómo la corte no solo habla de jueces cuando tocó el tema de la regulación de estas herramientas ya que trató de expandir la necesidad de un aparato judicial fuerte en materia de inteligencia artificial dando órdenes al Consejo Superior de la Judicatura para crear guías de apoyo y uso de nuevas tecnologías dentro de la rama judicial colombiana las cuales deben seguir ciertos estándares con los que se evite una posible vulneración de

derechos. Como se dijo anteriormente, la corte dio a distintos organos judiciales la tarea de implementar de manera responsable el uso de la inteligencia artificial dentro del trabajo propio de la rama, para esto además de dar órdenes, se han establecido una serie de principios que en ningún caso se deben violar ya que estos representan el eje central de la tarea de impartir justicia en Colombia, dichos principios determinados son:

I, Transparencia, II. Responsabilidad, III. Privacidad, IV. No sustitución de la racionalidad humana, V. Seriedad y verificación, VI. Prevención de riesgos, VII. Igualdad y equidad, VIII. Control humano, IX. Regulación ética, X. Adecuación a buenas prácticas y estándares colectivos, XI. Seguimiento continuo y adaptación XII. Idoneidad.

La rápida aceptación que esta innovación ha tenido dentro de la sociedad colombiana, ha dejado en evidencia el lento actuar de las autoridades y un intento incipiente por empezar a realizar una regulación.

EN EL CONTEXTO INERNACIONAL.

Ahora vamos a tratar casos internacionales y en donde vamos a abarcar el tema de la violación al derecho a la privacidad tratado desde diferentes puntos de vista, de como en otros países se está viendo vulnerado este derecho y que decisiones se toman al respecto o que medidas son la adecuadas cuando la tecnología nos afecta nuestro derecho a la privacidad. Cuando tratamos el tema sobre los derechos fundamentales siempre se nos viene a la mente hablar sobre la salud, el trabajo, la educación, entre otras consideraciones. Pero se nos olvida que cada vez más nuestro mundo está cambiando y está empezando la nueva era digital y con esta viene una serie de desafíos para la humanidad y por momentos pasa desapercibido que al introducirnos en esta era digital inconscientemente nuestra privacidad cada vez es más fracturada por los nuevos sistemas e implementaciones en este mundo digitalizado, En el primer caso, se abordará cómo una aplicación, originalmente desarrollada para proteger nuestra salud durante la pandemia de 2020, terminó comprometiendo gravemente nuestra

privacidad. En el segundo caso, se analizará cómo la instalación de cámaras de vigilancia en nuestro lugar de trabajo, sin nuestro consentimiento, constituye una grave vulneración de nuestro derecho a la privacidad y la intimidad.

Expediente N.º: PS/00222/2021, Agencia Española de Protección de Datos, 9 de junio de 2022, Aplicación RadarCovid

La Agencia Española de Protección de Datos (AEPD)[5] acordó el pasado 7 de septiembre de 2020 verificar si la app cumple con la normativa del Reglamento General de Protección de Datos, debido a varias noticia relativas a la protección de datos en la app RadarCOVID, la investigación se inició principalmente debido a la preocupación suscitada por varias denuncias contra La Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA)[6] que era la responsable del proyecto, estas denuncias se referían a cuestiones como la falta de transparencia, la protección de la intimidad de los usuarios y los fallos de seguridad. Fue en base a esto que la Agencia Española de Protección de Datos solicitó a SEDIA que aclarara una serie de aspectos en la aplicación RadarCOVID y que resolviera algunas dudas sobre el tratamiento que tienen esos datos. En concreto, solicitó información sobre varios temas: finalidad, licencias, medidas de seguridad, cumplimiento y participación de terceros. Por otro lado, la Agencia Española de Protección de Datos también ha investigado si se habían cubierto todos los requisitos sobre protección de datos y medidas de seguridad relativos a las App y APIs de Google y Apple, que se utilizaron en el desarrollo de RadarCOVID. En este sentido, la Agencia Española de Protección de Datos (AEPD) ha detectado varios problemas con la aplicación RadarCOVID en cuanto al tratamiento de los datos, la agencia ha encontrado lo siguiente:

1. No se llevó a cabo oportunamente una evaluación de impacto sobre la protección de datos, lo que podría exponer a los usuarios a riesgos que no habían considerado previamente.

[5] Agencia independiente de España que busca proteger los derechos de las personas en cuanto al manejo de datos personales se habla, su función es vigilar y asegurar el cumplimiento de la legislación sobre protección de datos.

[6] Organo del gobierno español encargado de desarrollar y promover la estrategia nacional de inteligencia artificial con el objetivo de posicionar a España como líder en este sector de la tecnología

2. El código fuente no se publicó de forma transparente, lo que dificultó la evaluación de la seguridad de la aplicación y la protección de la intimidad de los usuarios.

Sobre la base de la información facilitada, se adoptaron las siguientes decisiones y sanciones, en primer lugar, la Agencia Española de Protección de Datos decidió adoptar medidas correctoras contra la Secretaría de Estado de Digitalización e Inteligencia Artificial y ordenó que adecuara las operaciones de tratamiento de datos dentro de la app RadarCOVID a lo dispuesto en el Reglamento General de Protección de Datos y a las directrices del Consejo Europeo de Protección de Datos. En segundo lugar, se ordenó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) que aplique las recomendaciones necesarias para garantizar la seguridad y protección de los datos de los usuarios y subsane las deficiencias detectadas.

la famosa industria Amazon Inc. Fue multada por la Unión Europea debido a la violación de los derechos de privacidad de sus usuarios y también al mal manejo que se le da a estos datos, se dice la multa impuesta por la Unión Europea fue de 746 millones de euros, también grandes empresas como Google, Google ireland, Facebook, rappi y muchas empresas que a través de sus aplicaciones y paginas web al momento de regístrate violan los derechos de privacidad de sus usuarios.[7]

En la jurisdicción colombiana, cuándo se violan los derechos a la privacidad mediante alguna aplicación creada por estas grandes empresas ya mencionada se cuenta con mecanismos de protección del HABEAS DATA que mediante la sentencia T-307 de 1999[8], la Corte Constitucional ratificó esta distinción conceptual al afirmar que *"el hábeas data es un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectar, almacenar, usar y transmitirlo"*.

[7] Santos, C. (2024). Amazon recibe la mayor multa de la historia de la Unión Europea en materia de privacidad: 746 millones de euros por no cumplir con el RGPD. Xataka. https://www.xataka.com/privacidad/amazon-recibe-mayor-multa-historia-union-europea-materia-privacidad-746-millones-euros-no-cumplir-rgpd

[8] Sentencia que establece parámetros para el desarrollo del habeas data y su relación con el manejo de datos.

La privacidad se presenta como un tema complejo el cual enfrenta multifacéticos problemas, la cual no puede tener un solo eje ya que dependerá del contexto en el que se tome la manera en la que deba protegerse, por esto último se entiende que la privacidad puede estar sujeta una serie de riesgos tales como vigilancia, robo de datos y incluso la minería los cuales no deben ser atacadas con una legislación global sino más bien por entes individuales que entiendan cada contexto (Solove, 2008)

Juzgado de lo Social N°. 2 de Alicante/Alacant, Sentencia 190/2023 de 15 Sep. 2023, Rec. 489/2023

En este caso, un trabajador llamado Gabino demandó a su empleador, Albero Forte Composite, S.L., alegando una violación de sus derechos a la intimidad personal y a la propia imagen, debido a que la empresa había implementado un sistema para controlar las horas de entrada y salida de los empleados utilizando reconocimiento facial, pero esta no había obtenido el consentimiento explícito de Gabino para este uso específico de su imagen.

Hay que tener en cuenta que el señor Gabino había firmado previamente un consentimiento para que su imagen pudiera ser utilizada en materiales promocionales y publicitarios de la empresa, pero al señor nunca se le informó ni se le pidió autorización para que su imagen fuera utilizada en el sistema de control de asistencia basado en el reconocimiento facial. Además, la empresa en su ignorancia no llevó a cabo una evaluación de impacto en protección de datos, que llega a ser un requisito obligatorio cuando se utilizan datos biométricos, que llegan a ser considerados altamente sensibles.

Dos aspectos a tener en cuenta, el primero es analizar cómo se puede llegar a incurrir en un delito al afectar la privacidad de una persona o un trabajador si se lo está grabando sin su consentimiento y el otro problema es como el reconocimiento fácil y el simple uso de esta tecnología está afectando muy seriamente el derecho a la privacidad.

Hablando sobre la cuestiones de ser grabados sin nuestro consentimiento, para poder entender esto en la jurisdicción colombiana tenemos que definir qué es la intimida o la privacidad y para eso traemos la sentencia T-280-2022 que nos dice lo siguiente *"La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo,*

por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás y es una condición indispensable para el libre desarrollo de la personalidad". Es importante considerar que nuestro derecho a la privacidad puede ser vulnerado en diversos escenarios de nuestra vida cotidiana. Por ejemplo, al ingresar a un conjunto residencial, podemos ser grabados sin nuestro consentimiento, o al caminar por la calle, donde numerosas cámaras de vigilancia registran nuestras actividades. Sin embargo, en esta reflexión nos centraremos en un ámbito particular: el entorno laboral. Al llegar a nuestro lugar de trabajo, es posible que, sin nuestro previo consentimiento, el empleador o jefe nos grabe mientras desempeñamos nuestras labores. Esto constituye un grave problema, ya que la grabación sin nuestro consentimiento vulnera nuestro derecho fundamental a la privacidad. Además, este tipo de acciones puede tener repercusiones en nuestro futuro, ya que los videos grabados podrían ser utilizados de maneras que nos perjudiquen o incluso filtrarse, exponiendo aspectos íntimos de nuestra vida.

Resulta profundamente preocupante la idea de que, en la actualidad, parece que no estamos seguros en ningún lugar, debido a la omnipresencia de cámaras. Aunque estas pueden tener un propósito legítimo, como brindar seguridad o ayudar en la identificación de personas que cometen delitos graves, también tienen un lado oscuro. A medida que avanzamos en la era digital, se garantiza cada vez menos privacidad al ser humano dentro de la sociedad. Nuestros datos son recolectados y almacenados en servidores, muchas veces sin nuestro conocimiento o consentimiento. Aunque se nos asegura que estos servidores son seguros, cualquier falla podría resultar en la exposición de nuestros datos, acumulados durante días, meses o incluso años, a manos no deseadas. Esto revela lo frágil que se está volviendo nuestro derecho a la privacidad en un mundo cada vez más digitalizado.

El rápido avance de la tecnología está superando a los marcos jurídicos, especialmente en lo que respecta al reconocimiento facial. En un mundo donde la tecnología es esencial, la recolección de datos se ha vuelto omnipresente, a menudo transgrediendo la voluntad de las personas. Por esta razón, es crucial ser conscientes del manejo que se le da a nuestros datos y los riesgos que esto conlleva. Aunque el uso de nuevas tecnologías puede ofrecer innumerables beneficios, la falta de regulación adecuada puede, al mismo tiempo, abrir la puerta al desarrollo de amenazas significativas para la sociedad (Reyes, 2023).

TRIBUNAL EUROPEO DE DERECHOS HUMANOS, TERCERA SECCIÓN (Solicitud n.º 11519/20), 4 de julio de 2023

El caso de Glukhin contra Rusia ante el Tribunal Europeo de Derechos Humanos aborda la sanción administrativa impuesta a Nikolay Sergeyevich Glukhin, un ciudadano ruso, por participar en una manifestación en solitario sin notificar previamente a las autoridades. Durante su protesta, Glukhin utilizó una figura de cartón a tamaño real de un activista político, que las autoridades consideraron como un "objeto rápidamente ensamblable/desmontable" que requería notificación previa. La policía empleó tecnología de reconocimiento facial para identificar y rastrear a Glukhin, lo que facilitó su arresto. El Tribunal concluyó que el uso de esta tecnología puede disuadir a las personas de ejercer su derecho a expresar opiniones y afecta su privacidad. Además, determinó que la condena violaba tanto el derecho a la libertad de expresión (Artículo 10) como el derecho a la vida privada (Artículo 8) del Convenio Europeo de Derechos Humanos.

Se ha tratado cómo las cámaras de seguridad pueden violar el derecho a la privacidad, así como su capacidad para brindar seguridad en las ciudades. Sin embargo, ahora se quiere enfocar no solo en lo que capturan estas cámaras, sino en la implementación del reconocimiento facial. Este avance ha planteado un gran desafío para el ámbito jurídico, ya que aún no se ha logrado regular adecuadamente su función en las cámaras de seguridad que están presentes en la vida cotidiana.

Para abordar este tema, es importante destacar los aspectos positivos de este sistema, especialmente en términos de seguridad. Como se menciona en la sentencia, el reconocimiento facial se utilizó para identificar a una persona que estaba violando las normas jurídicas en Rusia. Este ejemplo ilustra cómo este sistema podría mejorar significativamente la seguridad al facilitar la identificación de delincuentes. Hoy en día, uno de los mayores desafíos es encontrar a las personas responsables de actos delictivos una vez que se han cometido. Con el reconocimiento facial, la búsqueda sería mucho más eficiente, permitiendo a la policía realizar capturas de manera más rápida y eficaz.

Desde un punto de vista negativo, la implementación del sistema de reconocimiento facial en las cámaras que vigilan los espacios públicos representa una clara violación del derecho a la privacidad. Este sistema es capaz de identificar y rastrear de manera eficiente todas las actividades cotidianas de las personas, como con quién se encuentran, qué están haciendo y en qué contexto lo están haciendo, todo ello a través del análisis de un patrón único: el rostro.

Este tipo de vigilancia constante afecta directamente la privacidad, ya que impide que las personas realicen sus actividades diarias sin ser observadas y sin que su comportamiento sea monitoreado. Aunque este sistema puede ser útil para mejorar la seguridad, también podría marcar el comienzo de la erosión del derecho a la privacidad, ya que convierte la vida cotidiana en un escenario de vigilancia constante.

Al analizar tanto los aspectos positivos como negativos del sistema de reconocimiento facial en las cámaras de seguridad ubicadas en espacios públicos, se reconoce que este avance puede mejorar significativamente la seguridad, permitiendo a las personas desplazarse con mayor libertad y reduciendo el riesgo de ser víctimas de robos o agresiones. En el peor de los casos, este sistema facilita la captura de delincuentes por parte de las autoridades.

Sin embargo, también es necesario considerar el costo de esta seguridad. La implementación de este sistema podría llevar a una vida en la que el derecho a la privacidad se vea comprometido. En el contexto del nuevo mundo digital en el que vivimos, es cada vez más difícil que este derecho sea respetado. Por ello, es crucial reflexionar sobre la necesidad de regular la tecnología, ya que, aunque puede ser una poderosa aliada, también tiene el potencial de convertirse en nuestro peor enemigo.

SENTENCIA T-294 DE 2023 CORTE CONSTITUCIONAL - Colombia agosto 3 de 2023

Desde 2003, la periodista y defensora de derechos humanos C.J.D.O. ha sido víctima de persecución, hostigamiento y tortura psicológica por parte de exmiembros del Departamento Administrativo de Seguridad (D.A.S.). En respuesta a estos actos de acoso, la Comisión Interamericana de Derechos Humanos (CIDH) le proporcionó un vehículo blindado y un grupo de escoltas para garantizar su protección y la de su familia, medios que son administrados por la Unidad Nacional de Protección (UNP).

En 2020, la periodista fue informada de un posible atentado en su contra, basado en el rastreo de sus desplazamientos mediante un GPS instalado en el vehículo blindado, según información proporcionada por la CIDH. También se le comunicó que algunas personas que habían formado parte de su esquema de seguridad mantenían contacto con exmiembros del D.A.S., lo que aumentaba su vulnerabilidad. Ante este conocimiento, en forma de protesta, la periodista decidió devolver el vehículo blindado a la UNP e interpuso una acción de tutela contra la UNP, alegando la afectación de su integridad y derechos fundamentales.

Sin embargo, la tutela fue rechazada en primera y segunda instancia, bajo el argumento de que el conocimiento de su paradero era esencial para garantizar su seguridad. A pesar de sus múltiples intentos por hacer valer sus derechos, la periodista presentó una denuncia contra la UNP, alegando la violación de su intimidad, privacidad, habeas data, y la re victimización de su situación. Asimismo, afirmó que nunca dio su consentimiento para dicho monitoreo y exigió la entrega de todos los datos recopilados por el GPS para su eventual destrucción. Por

su parte, la UNP respondió ante la corte que el monitoreo del GPS es una medida necesaria y aplicable a todos los vehículos bajo su control para asegurar la seguridad de los protegidos.

El asunto escala hasta la Corte Constitucional la cual analizó de la manera más idónea posible la posición de la víctima y se manifiesta frente a la misma teniendo en cuenta el artículo 15 de la Constitución Política que establece que *" toda persona tiene derecho a conocer la información que se haya recabado sobre ella en bancos de datos y en archivos de entidades públicas y privadas "*, así mismo, el artículo 8º de la Ley 1581 de 2012[9], estableciendo que *" por el principio de veracidad o calidad, el Titular tiene el derecho a conocer, actualizar y rectificar sus datos personales… Por el principio de transparencia, el Titular tiene derecho a conocer los datos que sobre él reposan en las bases de datos, solicitar prueba de la autorización brindada, ser informado del manejo que se ha hecho de sus datos y acceder de forma gratuita a sus datos personales."*

La UNP, por su parte, manifestó que su intención siempre ha sido proteger a las personas bajo su custodia, asegurando que la información recolectada a lo largo de los años se utiliza únicamente para implementar medidas de seguridad, y no con fines de inteligencia, contrainteligencia o seguimientos ilegales que puedan poner en riesgo a la persona protegida o a su círculo social.

Este caso plantea, por un lado, la responsabilidad de la UNP en la manipulación de los datos personales de la periodista, considerándolos elementos clave para garantizar su seguridad. Por otro lado, la víctima argumenta que el desconocimiento sobre el uso de sus datos personales la expone a un riesgo mayor, ya que estas acciones constituyen una invasión a su privacidad y autonomía. Ante esta situación, la Corte Constitucional buscó equilibrar las pretensiones y circunstancias de ambas partes, asegurando la protección de la víctima sin que la UNP transgreda sus derechos fundamentales. Este equilibrio entre el derecho y la integridad de las personas refuerza y mejora la protección de sus datos personales (Muñoz, 2014).

[9] Ley que busca desarrollar el derecho constitucional de los colombianos de poder actualizar, conocer y rectificar la información que repose en distintas bases de datos.

SAN 3693/2024 -ECLI:ESAN:2024:3693 - SAN A 04 de julio de 2024 -ROJ: SAN 36/2024- MADRID- FERNANDO DE MATEO MENÉNDEZ

El caso trata sobre una controversia de seguridad entre la aerolínea AIR EUROPA LÍNEAS AÉREAS S.A. y la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) en mayo de 2018, cuando un atacante accedió a la base de datos de la aerolínea, comprometiendo datos personales y financieros de los usuarios con fines fraudulentos. Como resultado, Air Europa fue multada con 600.000 euros por violar los artículos 32 y 33 del Reglamento General de Protección de Datos (GDPR).

El artículo 32 establece que el consentimiento para el tratamiento de datos personales debe ser un acto afirmativo claro que refleje una voluntad libre, específica, informada e inequívoca del interesado, mientras que el artículo 33 permite a los interesados dar su consentimiento para ámbitos específicos de investigación científica, incluso cuando no se pueda determinar completamente la finalidad en el momento de la recopilación.

En su defensa, Air Europa argumentó que las medidas de seguridad implementadas cumplían con los requisitos legales y que el GDPR no debería aplicarse retroactivamente, ya que la notificación del incidente a la AEPD se realizó fuera del plazo de 72 horas debido a una evaluación tardía del riesgo. Sin embargo, la Audiencia Nacional rechazó el recurso de Air Europa, afirmando que las medidas de protección adoptadas no fueron adecuadas para evitar el acceso no autorizado a los datos de los usuarios y que el aviso del incidente ya había prescrito. Además, consideró que las multas impuestas a la aerolínea no eran desproporcionadas.

Finalmente, la Audiencia Nacional confirmó las sanciones impuestas por la AEPD, concluyendo que las medidas de seguridad de Air Europa no fueron suficientes para evitar el acceso indebido a los datos personales de los usuarios.

Sentencia C-507/17 del tribunal de justicia de la Unión Europea.

Trata sobre al denominado "olvido" el cual construye la posibilidad de que quien lo desee pueda tener la posibilidad de borrar su historial de navegación en el momento en que así lo vea pertinente o necesario siendo este una de las mayores defensas para los derechos de

identidad y de intimidad, pero al mismo tiempo siendo un limitante para lo que el tribunal ha denominado como el derecho de carácter público a la información.

Este caso es de gran interés ya que involucra a Google Inc., una de las bases de datos más grandes del mundo, frente a la Comisión Nacional de Informática y Libertades de Francia (CNIL). El conflicto se centra en la solicitud de un particular para eliminar sus datos de ciertos motores de búsqueda, y la negativa del gigante tecnológico a llevar a cabo dicho proceso.

El tribunal abordó la sentencia desde dos esferas principales. Primero, evaluó cómo la solicitud de eliminación de datos por parte del demandante se relaciona con otras normativas previas sobre la gestión de datos personales, como la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995. Esta directiva se refiere a la protección de las personas físicas en relación con el tratamiento de sus datos personales y la libre circulación de estos.

A través de su análisis, el tribunal consideró que los datos personales pueden tener características especiales, reconociendo que algunos datos son más sensibles que otros y, por lo tanto, requieren un manejo más cuidadoso y una regulación más estricta para su almacenamiento y distribución. Dado el carácter delicado de ciertos datos, el tribunal subrayó la necesidad de reforzar las medidas de seguridad. Este factor fue clave para que el tribunal determinará en qué circunstancias los datos personales pueden ser eliminados por completo, y cuándo su eliminación podría afectar el interés público.[10]

La segunda esfera de interés en la sentencia, estrechamente relacionada con lo mencionado anteriormente, se centra en lo que podría denominarse el equilibrio o ponderación de derechos. Este concepto se refiere al conflicto que surge cuando un individuo desea ejercer control sobre su propia información, mientras que el sector público busca acceso a la misma. Como resultado, la decisión del tribunal genera opiniones divididas. Aunque se reconoce que cada persona tiene el derecho de gestionar sus datos de acuerdo con sus intereses, se estipula

[10] Normativa que representó un hito en la protección de datos dentro de la Unión Europea, establece requisitos para el tratamiento seguro de datos como el consentimiento, la exactitud y la transparencia.

que las entidades que custodian dichos datos deben evaluar cada solicitud de eliminación con sumo cuidado. Estas solicitudes deben estar respaldadas por una justificación sólida, ya que los datos en cuestión podrían ser de gran interés público, un interés que podría prevalecer sobre los derechos individuales, incluso en asuntos relacionados con el acceso a la información.

Para lograr este equilibrio, el tribunal establece parámetros que los repositorios de datos deben seguir al evaluar cada solicitud, con el objetivo de evitar rechazos poco éticos o arbitrarios. Más allá de la ponderación de derechos en este caso, la sentencia traza un camino hacia un mayor entendimiento del manejo individual y colectivo de los datos. Sin embargo, el fallo deja abierta la posibilidad de que la gestión de los datos personales quede en manos de grandes motores de búsqueda, sin una regulación adecuada, y basada únicamente en el concepto de interés público.

Además, la sentencia revela una realidad inquietante y a menudo ignorada: en el mercado global actual, el producto más codiciado ya no es la última innovación tecnológica, sino nuestros datos personales. Esta información, que abarca desde nuestros hábitos de compra en línea hasta nuestro historial médico o crediticio, se ha convertido en un bien altamente valorado. Si reflexionamos sobre esto, resulta evidente la necesidad urgente de que las autoridades de todas las naciones implementen un plan de acción para regular y controlar este creciente mercado de datos. De lo contrario, se corre el riesgo de dejar la información sensible de las personas a merced de la arbitrariedad. El derecho al olvido no debe ser visto como una herramienta para reescribir la historia, sino como un medio para proteger a las personas de ser juzgadas injustamente por la permanencia digital de sus acciones pasadas (Floridi, 2020).

DPC-1001, Caso META y GDPR, la decisión irlandesa.

En el año 2023, en el marco de la protección de datos electrónicos la Comisión de Protección de Datos de Irlanda llevó a los tribunales a Meta Platforms Ireland Limited, en un caso que revolucionó el sector de la regulación de la privacidad de datos en un contexto global. La decisión, que sentó un precedente se fijó en 1.2 millones de euros siendo así la multa más alta hasta la fecha bajo la tutela del Reglamento General de Protección de Datos GDPR así como también la imposición de carácter inmediato de detener la transferencia de datos desde

la Unión Europea hacia los Estados Unidos lo cual representaba una violacion grave al derecho a la intimidad de los usuarios de la plataforma.

Además de centrarse en el tema de la protección en contra de la transferencia de datos, el caso basó su actuar en el fallo Schrems II del Tribunal de Justicia de la Unión Europea en 2020[11] el cual dejaba sin efectos el Escudo de Privacidad que existía entre Estados Unidos y la Unión Europea lo que dejó a muchas empresas del sector tecnológicas en una especie de vacío legal obligándolas a depender de Cláusulas En contratos de tipo SCC[12] lo que les daba la posibilidad de continuar con la migración de Datos, la relación que existe entre ambas decisiones terminó reflejando fue la floja protección que tenía Meta para con los datos que transfería así como también la poca regulación que tiene el sector en los Estados Unidos.

El pasó utilizado por la DPC[13] fue determinar qué Meta estaba infringiendo el Artículo 46/1 del GDPR el cual establece unos parámetros de seguridad mínimo para poder realizar migración de datos por fuera de la Unión Europea con la idea de brindar seguridad a los usuarios. Dentro del análisis realizado se llegó a la conclusión de que las cláusulas del tipo SCC representan un riesgo dentro de la protección de datos sobretodo aplicado en un contexto de un estado receptor como lo es Estados Unidos el cual dispone de estamentos legales que permiten la vigilancia estricta e intrusiva sin protección ninguna en los datos que llegan desde la Unión Europea. La decisión a la que se llegó no solo se limitó a castigar la infracción de Meta, sienta un precedente al encontrar las deficiencias en los mecanismos de vigilancia en la transferencia de datos lo cuales se ven fragmentados cuando se aplican en naciones en donde las prácticas de cuidado a los datos tiene una base muy débil como lo es Estados Unidos, lo que al final se logró fue abrir una puerta a que en el futuro se creen regulaciones y estamentos encargados de incrementar los niveles de seguridad a nivel global respecto al tratamiento que se le debe dar a los datos electrónicos de las personas resultando así en una

[11] La sentencia del Tribunal de Justicia de la Unión Europea (TJUE) emitida el 16 de julio de 2020, la cual daba por terminado el marco de protección de datos conocido como Escudo de Privacidad (Privacy Shield), el cual permitía transferir datos desde la Unión Europea hasta Estados Unidos

[12] Disposiciones estandarizadas en contratos las cuales garantizan que la transferencia de datos del espacio aéreo de la UE se haga fuera de este según las reglas de la GDPR.

[13] Comisión de protección de datos de Irlanda, encargada de vigilar e investigar quejas relacionadas con temas de violación de privacidad electrónica.

configuración significativa que proteja la privacidad y la coloque como prioridad número uno.

Pará efectos prácticos la multa de 1.2 millones de euros no es solo una sanción de carácter financiera, representa también una declaración de principios la cual pone fin a una preocupación mundial sobre la capacidad de las grandes empresas del sector tecnológico para evadir, mitigar y de plano desconocer los reglamentos sobre transferencia de datos ya que además de, perjuicio económico, Meta recibió la orden de suspender las transferencias futuras hacia Estado Unidos en un plazo de 5 meses para así poder alinear lo que dispuso la GDPR con las bases de almacenamiento de datos. Además de ser un golpe a las finanzas de meta es un cambio en la relación de poder entre los reguladores y las corporaciones de tecnología. Pone de presente dos panoramas totalmente diferentes para el actuar de las corporaciones, Por un lado, antes hacían uso de las cláusulas SCC las cuales permitían crear Mecanismos propios susceptibles de fallos siendo este un ataque a la privacidad de sus usuarios y otro con la vigilancia de la DPC la cual actúa como garante para los derechos de aquellos que depositan su información en distintas bases de datos.

Ahora bien, la decisión del fallo no sólo entra a afectar a Meta, de manera indirecta son otras empresas que operan en diferentes jurisdicciones las que sienten su efecto ya que también se verán obligadas a reevaluar sus prácticas de transferencia de datos, esto bajo la consigna de ser objetos de futuras sanciones que pueden ser de tipo financiero las cuales incluso podrían ser mucho más severas que la de Meta e incluso llegando a la suspensión de actividades.

El fallo es una muestra clara de la creciente te preocupación que tienen las autoridades europeas las cuales cuentan con las herramientas para imponer justicia en los casos en que la violación de la privacidad, todo con la intención de dar garantías a las personas que han dispuesto las bases de datos de las corporaciones tecnológicas como el repositorio final de su información. Con el paso del tiempo el mundo digital evoluciona a pasos agigantados y la decisión de este fallo puede ser el pilar que marque el inicio de una era en donde lo que prime sea la soberanía de los datos haciendo que estos no sean Solo parte de la privacidad de la esfera de la persona sino también su origen.

El análisis realizado en este artículo revela varias conclusiones clave sobre las implicaciones jurídicas de la inteligencia artificial en el derecho informático, la seguridad informática y la privacidad. En primer lugar, se destaca la insuficiencia de la legislación actual en muchas jurisdicciones para abordar los desafíos únicos que plantea la IA, lo que subraya la necesidad de una reforma regulatoria. En segundo lugar, los resultados muestran que, aunque la IA ofrece grandes beneficios en términos de eficiencia y seguridad, también presenta riesgos significativos, especialmente en relación con la privacidad y los derechos fundamentales. Finalmente, se identifican diferencias significativas en los enfoques regulatorios entre diferentes países, lo que sugiere la necesidad de una mayor armonización a nivel internacional para asegurar que los derechos de los individuos estén protegidos de manera consistente.

La protección de datos en el contexto de la inteligencia artificial es un área donde se han identificado importantes deficiencias. Aunque existen regulaciones como el GDPR que establecen estándares elevados para la protección de datos, muchas jurisdicciones carecen de marcos legales comparables. Incluso en lugares donde existen regulaciones robustas, la aplicación de estas leyes en relación con los sistemas de IA presenta desafíos significativos.

Los casos de estudio analizados en este artículo proporcionan ejemplos concretos de cómo la inteligencia artificial está siendo implementada y los desafíos legales que esta implementación plantea. Representan para el objeto de estudio del presente una forma de análisis práctica con la que se puede estudiar como el uso de los distintos motores de inteligencia artificial han dado paso a lo largo del tiempo a la creación de distintos vacíos de tipo legal que pueden dejar como resultado el desarrollo de nichos perfectos para la creación de delitos digitales los cuales al no tener una regulación efectiva por parte de los sistemas legales pueden significar un peligro constante no sólo para las personas del común, sino también para los sistemas de gobierno de incluso las naciones más poderosas del mundo.

La comparación de resultados entre diferentes jurisdicciones revela una variabilidad significativa en la forma en que los países están abordando la regulación de la inteligencia artificial.

El impacto de la inteligencia artificial en la privacidad de los usuarios es una de las preocupaciones más críticas identificadas en este análisis. La capacidad de los sistemas de

IA para recopilar, analizar y correlacionar grandes volúmenes de datos personales plantea serios riesgos para la privacidad. Por ejemplo, el uso de IA en plataformas de redes sociales ha permitido la creación de perfiles detallados de los usuarios, que pueden ser utilizados para influir en su comportamiento o para tomar decisiones automatizadas que les afecten directamente, como la personalización de anuncios o el filtrado de contenido. Estos riesgos se ven amplificados por la falta de transparencia en muchos sistemas de IA, lo que dificulta que los usuarios comprendan cómo se utilizan sus datos y que puedan ejercer un control efectivo sobre ellos. La regulación de la IA debe abordar estas preocupaciones garantizando que los derechos de privacidad de los usuarios estén protegidos y que exista una supervisión adecuada para evitar abusos.

La jurisprudencia analizada en este artículo proporciona importantes lecciones sobre cómo los tribunales están respondiendo a los desafíos legales que plantea la inteligencia artificial. En muchos casos, los actores judiciales han mostrado una disposición a aplicar principios legales tradicionales a situaciones nuevas y complejas creadas por la IA, como en casos de privacidad y protección de datos. Sin embargo, también se ha identificado una falta de consistencia en las decisiones jurídicas, lo que sugiere la necesidad de desarrollar un marco jurisprudencial más coherente y adaptado a las especificidades de la IA.

La protección de los derechos fundamentales en el contexto del creciente desarrollo de la inteligencia artificial es un tema de vital importancia que debe ser abordado de manera urgente. La IA tiene el potencial de impactar negativamente en derechos como la privacidad, la no discriminación y la libertad de expresión si no se regula adecuadamente. Por ejemplo, los sistemas de reconocimiento facial pueden ser utilizados para la vigilancia masiva, lo que podría violar el derecho a la privacidad y fomentar la discriminación si los algoritmos utilizados no son imparciales. Asimismo, la toma de decisiones automatizadas en áreas como el empleo o la justicia penal podría llevar a la perpetuación de sesgos existentes o incluso a la creación de nuevos. Este artículo argumenta que es esencial que las leyes y regulaciones se diseñan para proteger estos derechos fundamentales, asegurando que la tecnología se utilice de manera que respete la dignidad humana y promueva la equidad y la justicia social.

CONCLUSIONES.

Este artículo ha explorado de manera exhaustiva las implicaciones jurídicas de la inteligencia artificial en el derecho informático, la seguridad informática y la privacidad. A lo largo del análisis, se ha identificado que la legislación actual es insuficiente para abordar los desafíos únicos que plantea la IA, lo que subraya la necesidad de reformas significativas en los marcos regulatorios existentes. Además, se ha destacado que, si bien la IA ofrece grandes beneficios, como la mejora de la eficiencia y la capacidad de resolver problemas complejos, también presenta riesgos significativos, especialmente en relación con la privacidad y los derechos fundamentales. La necesidad de un enfoque regulatorio adaptativo y ético es un tema recurrente que ha sido subrayado en cada sección del análisis.

En el ámbito de la seguridad informática, la inteligencia artificial tiene el potencial de tanto mejorar como comprometer la seguridad de los sistemas. Si bien la IA puede ser una herramienta poderosa para detectar y prevenir ciberamenazas, también puede ser utilizada para desarrollar ataques más sofisticados. Este doble filo subraya la necesidad de establecer normativas de seguridad que sean tanto preventivas como reactivas. La privacidad y la protección de la intimidad se han visto significativamente afectadas por la proliferación de tecnologías de inteligencia artificial. La capacidad de la IA para recopilar, analizar y correlacionar datos personales presenta riesgos sin precedentes para la privacidad de los individuos. Este artículo concluye que es imperativo reforzar las leyes de protección de datos, no solo para cubrir las brechas existentes, sino también para anticipar futuros desafíos relacionados con el desarrollo de la IA.

La jurisprudencia juega un papel fundamental en la configuración de cómo se interpretan y aplican las leyes en el contexto de la inteligencia artificial. Este artículo ha demostrado que, aunque los tribunales han comenzado a abordar cuestiones relacionadas con la IA, todavía existe una considerable incertidumbre sobre cómo se deben manejar casos complejos que involucran tecnología avanzada. La falta de precedentes claros y consistentes subraya la necesidad de un mayor desarrollo jurisprudencial que pueda proporcionar una guía más sólida tanto para los desarrolladores de IA como para los legisladores. Este artículo concluye que es crucial que los tribunales adopten un enfoque proactivo para resolver las lagunas

legales y que estén dispuestos a adaptar las interpretaciones legales tradicionales a las nuevas realidades tecnológicas.

CAPÍTULO 2

LOS DERECHOS DE AUTOR EN LOS SISTEMAS MUSICALES DEL SIGLO XXI, UNA ALTERNATIVA DESDE EL CONTEXTO LOCAL E INTERNACIONAL COLOMBIANO.

Autores:

Yuri Luceny Diaz Chamba

Germán Esteban Oyola Meneses

Gissela Quiñoes Valencia

RESUMEN.

El trabajo estudia la manera con la que las nuevas tecnologías especialmente la inteligencia artificial han cambiado a la industria musical exponiendo a los artistas a una serie de riesgos relacionados con la violación de la propiedad intelectual.

Se ha analizado el marco legal colombiano destacando leyes como la 23 de 1982 así como también regulación de orden internacional como el convenio de Berna. Se señala además como en Colombia se ha dejado un poco de lo la protección de las obras musicales dentro de la era digital y la necesidad latente que existe de actualizar el marco normativo que sean fuertes a la hora de hacer frente a estos nuevos retos y se hace mención a la creación de derechos de tipo editorial y fotográfico además de la implementación de licencias que regulen el uso de algoritmos musicales con el fin de que la protección de los intereses de los creadores sea efectivo.

DELIMITACION DEL PROBLEMA.

En materia de propiedad intelectual y de los derechos de autor respecto de uno de los campos de estudio con poca profundización como son los algoritmos musicales, los cuales permiten la creación de música a través del uso adecuado y combinación de diferentes notas, siendo esta una actividad que se pone en riesgo si se tiene en cuenta que quienes componen estas obras musicales, se ven expuestos a que otras personas puedan utilizar sin reconocimiento de la propiedad intelectual estos algoritmos.

Frente a lo anterior se encuentra que con el pasar de los años diferentes organizaciones han impulsado el desarrollo de convenios internacionales que permitan generar una protección efectiva a los derechos de autor o de propiedad intelectual, entre los cuales se encuentran el convenio de Berna el cual está dirigido a la protección de las obras literarias y artísticas mismo que fuese aprobado por la ley 33 de 1987, de igual forma se encuentra la convención de Roma, 1961 convención internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión, así como el tratado sobre el registro internacional de obras audiovisuales, adoptado en Ginebra el 18 de abril de 1989, conferencia diplomática sobre ciertas cuestiones de derecho de autor y derechos conexos en la cual se aprueba el tratado de la OMPI sobre interpretación o ejecución y fonogramas mismo que se encuentra contenido la ley 545 de 1.999.

El derecho de autor o derecho a la propiedad intelectual no es solo una inquietud que nace con la sociedad postmodernista, Herrera (2021) citando a Marco Vitruvio indica que este tomaba este concepto en su Libro Séptimo, de arquitectura, diciendo:

> Ahora bien, así como hay que tributar merecidas alabanzas a éstos, incurren en nuestra severa condenación aquellos que, robando los escritos a los demás, los hacen pasar como propios. Y de la misma manera, los que no sólo utilizan los verdaderos pensamientos de los escritores, sino que se vanaglorian de violarlos, merecen reprensión, incluso un severo castigo como personas que han vivido de una manera impía (p.67).

Estos aspectos relacionaban el progreso de la sociedad a la creación y búsqueda de conocimiento de ciertos autores y se les buscaba el derecho moral sobre su obra, sobre todo literaria. Pese a ello y con la aparición de la imprenta surge la eventualidad de proteger no un solo objeto como propiedad material, sino sus múltiples reproducciones como fuentes de propiedad intelectual. De esta manera el Estado inicio con el control a las producciones con un doble fin:

- Primero: proteger a quienes invertían en la difusión de obras
- Segundo: controlar esta nueva fuente de oposición al poder.

Es así que para el año de 1710 se concede el primer género de protección formal al derecho de autor a través del Estatuto de la Reina Ana de Inglaterra (1762), crea el derecho exclusivo a imprimir (Pabón, 2009).

El derecho de autor en Colombia emprendió a ser reglamentado desde el año 1834, bajo el gobierno del General Francisco de Paula Santander se consignó la primera ley sobre el tema, mediante la ley 10 del mismo año, la cual reconoció a los nacionales y extranjeros residentes en él. Según Pérez (2013) el territorio del Estado el derecho exclusivo de imprimir, grabar, litografiar y reproducir, de cualquier otra manera semejante, las obras, composiciones literarias, los mapas, planos o pinturas, diseño o dibujos, y las composiciones musicales de que fuesen autores, siempre que dicha publicación se haga dentro de la Nueva Granada. El derecho de autor asumió sus orígenes a partir de un carácter material y territorial y sólo se registraba dentro del territorio nacional pues al referirse a obras literarias el idioma suponía una barrera.

> Sin embargo, tomando en cuenta la universalidad de las obras del espíritu cuya explotación traspasa las fronteras físicas se vio la necesidad de proteger el intercambio cultural de modo que se preservase tanto los derechos morales como patrimoniales

> del autor. Así en 1886, se firmó el Convenio de Berna para la protección de obras literarias y artísticas constituyéndose en la fuente internacional de protección del derecho de autor (Pérez, 2010, p. 3)

La protección igualmente incluye derechos morales que equivalen al derecho de reivindicar la autoría de una obra y al derecho de oponerse a modificaciones de la misma que pueden atentar contra la reputación del creador. La propiedad intelectual de acuerdo a la enunciación de la Organización Mundial de la Propiedad Intelectual, es toda creación, generación o producción del intelecto humano, según esta institución los derechos de propiedad intelectual salvaguardan los intereses de los autores al ofrecerles privilegios en relación con sus creaciones (Eafit, 2024)

Según la Organización Mundial de la Propiedad Intelectual (OMPI) (2023), de acuerdo a lo expuesto anteriormente se encuentra que la propiedad intelectual incluye dos categorías:

La propiedad industrial: Este aspecto hace referencia a las invenciones, patentes, marcas, dibujos y modelos industriales e indicaciones geográficas. Este derecho es exclusivo y lo otorga el Estado para usar o explotar en forma industrial y comercial las invenciones o innovaciones de aplicación industrial o indicaciones comerciales que realizan individuos o empresas para distinguir sus productos o servicios ante la clientela en el mercado.

El derecho de autor: esta abarca las obras literarias y artísticas, tales como las novelas, los poemas y las obras de teatro, las películas, las obras musicales, las obras de arte, como los dibujos, pinturas, fotografías y esculturas, y los diseños arquitectónicos (Organización Mundial de la Propiedad Intelectual – OMPI, 2023)

Los anteriores fundamentos teóricos evidencian la importancia que tiene el tema de derechos de autor y protección de la propiedad intelectual, encontrando que en Colombia dentro del Código Civil (1873), este se incluye en el capítulo de la necesidad que se tiene frente al reconocimiento de los bienes incorporales (artículo 653), donde se incluyen las producciones del talento o del ingenio o de propiedad de sus autores (artículo 671).

Con la entrada en vigencia de la Constitución Política de 1991, se llevó a cabo un replanteamiento sobre lo concerniente a los derechos de autor y se estableció el deber que tiene el Estado frente a su protección, así las cosas y con ley 32 de 1886 se buscó generar una visión clara sobre lo que es propiedad literaria y artística, definiendo el derecho de autor como «la facultad que las leyes reconocen a los autores durante un tiempo determinado y previas ciertas formalidades, para explotar sus obras» (artículo 1°), y fijó un monopolio por la vida del autor y 80 años más (artículo 10). La anterior reglamentación seria derogada por la ley 86 de 1946 y ésta a su vez por la ley 23 de 1982, de manera posterior y para el año 1988 se firmó el Convenio de Berna y el Tratado WCT, siendo estos dos, parte del acuerdo subregional Andino, sobre el Derecho de Autor y Derechos Conexos (OMPI, 2016).

Respecto del tema de la presente investigación es importante analizar aquellas causas que han llevado a una inadecuada utilización de los denominados ALGORITMOS MUSICALES, siendo esto una afectación directa al patrimonio de los artistas que con su labor generan obras musicales que fácilmente se ven expuestas a su violación de propiedad intelectual, esto debido básicamente a la continuada evolución de medios tecnológicos que permiten una fácil manipulación, intercambio y alteración de archivos digitales, trayendo consigo el incremento de la piratería y la aparición de novedosas formas de delito que ponen en peligro los derechos de autor, que obligan al mercado y a los artistas a buscar nuevas dinámicas de venta y de difusión de la música. Sin embargo, es necesario aclarar que el problema en el uso de los algoritmos musicales era poco relevante hasta el momento en que se popularizó la inteligencia artificial, por la falta de un ordenamiento jurídico que la regule actualmente (Valencia, 2023).

Es así que en el mercado colombiano de la música y en particular aquella que se encuentra alojada en sitios de internet legales e ilegales, se encuentra que estos permiten descargar títulos inclusive sin consentimiento alguno de sus creadores afectando a la industria en general, pues los productores de fonogramas, al darse cuenta de que el formato físico ya no genera las ventas de los ochenta, están iniciando su participación en la red, llevando a su exposición de ser pirateados en descargas que no cancelan valor alguno por sus producciones. Un dato de especial relevancia suministrado por la Dirección Nacional de Derecho de Autor Colombia (2024) sobre los registros de obras musicales de los dos últimos años:

DEPARTAMENTO	No DE INSCRIPCIONES 2022	No DE INSCRIPCIONES 2023
CUNDINAMARCA	6.823	6.681
ANTIOQUIA	4.261	4.045
VALLE DEL CAUCA	1.708	1.644
ATLANTICO	1.200	1.286
BOLIVAR	1.116	824
CESAR	723	789
SANTANDER	685	693
CÓRDOBA	380	533
RISARALDA	338	SIN INFORMACIÓN
SUCRE	521	SIN INFORMACIÓN
CALDAS	323	SIN INFORMACIÓN
RISARALDA	507	SIN INFORMACIÓN

Fuente: Dirección Nacional de Derecho de Autor Colombia. (2024). Registros de obras musicales.

La información anterior evidencia que durante el 2023 existido un leve descenso frente al registro de las obras musicales, entre las cuales se encuentran los siguientes géneros:

1. REGGAETON 1299	1. CORRIDO 719	1. ROCK 454	1. CHAMPETA 366
2. VALLENATO 1434	2. SALSA 661	2. RANCHERA 472	2. PASEO 348
3. POPULAR 1271	3. SALSA 645	3. CUMBIA 415	3. INSTRUMENTAL 362
4. POPULAR 1187	4. BALADA 588	4. PASEO VALLENATO 443	4. RAP 341
5. POP 980	5. BALADA 625	5. PASEO 383	5. VALS 360
6. REGGAETON 1077	6. CORRIDO 573	6. INSTRUMENTAL 404	6. ELECTRONICA 324
7. VALLENATO 855	7. RANCHERA 532	7. BAMBUCO 375	7. POP LATINO 352
8. POP 953	8. ROCK 571	8. BAMBUCO 393	8. ROCK ALTERNATIVO 321
9. URBANO 770	9. PASEO VALLENATO 477	9. CLASICA 369	9. RAP 339
10. URBANO 682	10. CUMBIA 540	10. HIP-HOP 388	10. CHAMPETA 293

Por ejemplo, la información anterior muestra que el ritmo musical con el mayor número de solicitudes es el VALLENATO con 1434 solicitudes de registro, seguido de REGGAETONM con 1299 y en tercer lugar la música POPULAR con 1271 registros.

En ámbito mundial la Federación Internacional de la Industria Discográfica, de la cual hacen parte más de 1.450 compañías productoras de fonogramas de 75 países en los cinco continentes, informó en su reunión anual en Londres que uno de cada tres discos que se

venden alrededor del mundo es una copia ilegal (Lizecita, 2023). Siendo este un escenario que anualmente genera ventas pitaras de música que superan los 4.6 billones de dólares, lo cual se convierte en un problema alarmante y de afectación patrimonial para las personas que trabajan para la industria musical.

Conforme de lo anterior el problema en la industria de la música y en particular frente a los retos y novedades en el sistema, es básicamente que los gobiernos no cuentan con una regulación clara, universal y efectiva en materia protección de estos derechos, de ahí que surge la necesidad de establecer e identificar retos y novedades derivados de las nuevas tecnologías frente a la protección de propiedad intelectual en los derechos de autor.

ARGUMENTACION.

Sistema clásico: Los antecedentes del sistema clásico del registro musical referente a la protección de su propiedad intelectual se remontan al año 1777 en Europa, concretamente en Francia, donde el conocido dramaturgo Beaumarchais, se propuso impulsar una organización que buscaba proponer por los derechos intelectuales de los autores.

Lo anterior presta atención a la Declaración Universal de los Derechos Humanos. Concretamente en 1948 cuanto en su artículo 27 se consideran derechos humanos, esto frente a la especial protección de los intereses morales y materiales del autor.

Es así que, en 1791, finalmente, la Asamblea Nacional aprobó la primera ley de derechos de autor, para luego dar paso en el año de 1886 con la firma del Convenio de Berna, en la cual se establecieron los criterios para la protección de la propiedad intelectual, derechos de autor y los compromisos que tienen los países participantes a proteger estos derechos mediante sus legislaciones nacionales.

Sistema moderno: En la actualidad los derechos de autor y de propiedad intelectual de la música se encuentran contenidos en las diferentes legislaciones alrededor del mundo, esto bajo las premisas de los tratados internacionales que los diferentes Estados han suscrito a lo largo de la historia como lo es el virtud del Convenio de Berna para la protección de las Obras

Literarias y Artísticas, celebrado en 1886 y administrado por la Organización Mundial de la Propiedad Intelectual (OMPI), en la cual se establecer que una obra original goza de protección durante al menos 50 años después de la muerte del autor, pero en muchos territorios ese periodo puede ser de 70 años o más.

En la organización OMPI, se encuentra la legislación en materia de derecho de autor respecto de las obras originales, así como la protección que tienen aquellos quienes las interpretan o ejecutan, o a los encargados de su difusión generalizada (por ejemplo, las compañías discográficas y los organismos de radiodifusión). La norma relativamente indica que:

La protección por derecho de autor entra en vigor en cuanto la obra es creada, es decir, en cuanto existen una música, una letra, unos arreglos o una grabación. No existe la obligación formal de registrar la obra ante una autoridad nacional, aunque en algunos países, como los Estados Unidos de América, el registro de la obra en la Biblioteca del Congreso es la única vía para presentar una demanda judicial en caso de infracción (OMPI, 2024).

Legislación aplicable a los algoritmos musicales en la música contemporánea

A continuación, se presentan el marco normativo aplicable en la actualidad a nivel de derechos de autor y de propiedad intelectual:

NORMAS.

En el ámbito nacional se encuentra que, respecto de la política de protección sobre la propiedad intelectual y derechos de autor, están las siguientes:

En materia de Derechos de autor

Constitución Política de Colombia de 1886: Sólo tutela el derecho de autor, dejando su regulación especial a la ley.

Constitución Política de Colombia: En el artículo 61 de la Constitución establece que el "Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que

establezca la ley." Este mandato implica, de acuerdo con la jurisprudencia constitucional, que la propiedad intelectual y sus derechos conexos son inalienables.

Ley 23 de 1982: Los fundamentos normativos que establece esta ley están dirigidos a la protección de obras literarias, artísticas y científicas, mismas que resultan no ser objeto de apropiación. Su contenido exalta del deber que tiene el Estado por brindar protección exclusiva a la forma literaria, plástica o sonora, y como estas deberán ser descritas, explicadas, ilustradas o incorporadas en las obras literarias, científicas y artísticas.

Ley 44 de 1993: Esta norma modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944, esta tiene como finalidad, armonizar la normativa nacional frente a las obligaciones asumidas por el Estado frente a aquellas suscripciones de diferentes tratados internacionales, con la inclusión de cinco capítulos relativos al Registro Nacional de Derecho de Autor, las sociedades de gestión colectiva de derecho de autor y derechos conexos, el tratamiento del derecho de autor para los servidores públicos, y un capítulo de disposiciones penales (Capítulo IV titulado. De las sanciones).

Ley 232 de 1995: En esta norma se fija una exigencia económica a aquellos establecimientos comerciales donde se reproduzcan obras musicales, esto en concordancia a lo contenido en la Ley 23 de 1982 y demás normas complementarias.

Ley 1403 de 2010: Por la cual se adiciona la Ley 23 de 1982, sobre Derechos de Autor, se establece una remuneración por comunicación pública a los artistas, intérpretes o ejecutantes de obras y grabaciones audiovisuales o "Ley Fanny Mikey".

Ley 1834 de 2017: También conocida como Ley Naranja, busca promover una participación coordinada institucional frente a la protección de la propiedad intelectual, y la protección de los derechos de los creadores, así como a la generación de inclusión de internacionales para enfrentar la piratería.

Ley 1835 de 2017: por la cual se modifica el artículo 98 de la ley 23 de 1982 "sobre derechos de autor", se establece una remuneración por comunicación pública a los autores de obras cinematográficas o "Ley Pepe Sánchez". Con la cual se establecer aquellos derechos patrimoniales sobre la obra cinematográfica, así como genera un marco de regulación sobre la cesión de los derechos de los autores, el derecho a una remuneración equitativa y que dicha

remuneración no es aplicable a aquellos establecimientos abiertos al público que utilicen la obra audiovisual para entretenimiento de sus trabajadores.

Ley 1915 de 2018: Fina disposiciones sobre protección de derechos de autor en el entorno digital, contenidas en el capítulo de propiedad intelectual del TLC. De igual forma compromete a los Estados en torno a la abolición de jerarquías entre los derechos de autor y derechos conexos.

Decreto 1360 de 1989: Reglamenta la inscripción de soporte lógico (software): Por el cual se reglamenta la inscripción de soporte lógico en el Registro Nacional del Derecho de Autor". Protegiendo en especial lo que se denomina el programa de computador, la descripción de programa y el material auxiliar. De lo cual se desprenden derechos morales que siempre le pertenecerán al creador y los patrimoniales sobre su explotación y comercialización.

Decisión 351 de 1993 de la Comunidad Andina de Naciones. Tiene como objetivo brindar una protección a los autores y a otros titulares de derechos sobre obras de tipo literario, artístico o científico, así mismo, se protegen los derechos conexos.

Convenio de Berna de 1989: Establece los mecanismos de protección a obras artísticas y literarias, esto en aspectos legales, contexto y les permite a los Estados parte determinar qué componentes son susceptibles de ser considerados materia de protección ya sea por acción judicial, administrativa, u legislativa.

Convención de Roma de 1961: Se identifica como una convención internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión. Históricamente esta convención brinda un primer acercamiento a la etimología de fonograma, introduciendo el concepto de este como escritura o grabación de sonido y definiéndolo como: “Toda fijación exclusivamente sonora de los sonidos de una ejecución o de otros sonidos” (Artículo 3b).

Tratado sobre el Registro Internacional de Obras Audiovisuales: Lo que se busca con este tratado es el de incrementar la seguridad jurídica de las transacciones relativas a las obras audiovisuales, así como el de promover la creación de obras audiovisuales, intercambios internacionales de obras y de contribuir a la lucha contra la piratería.

Tratado de la OMPI sobre Derechos Conexos de 1996: Este tratado adoptado en virtud del Convenio de Berna, habla sobre la protección de las obras y los derechos económicos de sus autores en el entorno digital. El también busca proteger i) los programas de computadora, con independencia de su modo o forma de expresión, y ii) las compilaciones de datos u otros materiales.

EN MATERIA DE PROPIEDAD INDUSTRIAL.

Ley 603 de 2000: Por la cual se modifica el artículo 47 de la Ley 222 de 1995. Conocida como la ley de licencias de Software (o Ley para cumplimiento de las licencias de Software). Esta normatividad se establecen las sanciones penales a las cuales se puede llegar respecto de la violación de la propiedad intelectual y derechos de autor, norma que contempla penas de prisión de 2 a 5 años y multas de 20 hasta 1000 salarios mínimos legales mensuales vigentes.

Decisión 486 de 2000 de la Comunidad Andina de Naciones: Contiene normas de obligatorio cumplimiento sobre la protección de la propiedad industrial para los países miembros de la Comunidad Andina, de la Organización Mundial del Comercio y del Convenio de París para la Protección de la Propiedad Industria. Lo cual busca generar una protección especial a los elementos de la propiedad industrial, salvaguardando y respetando su patrimonio biológico y genético, así como los conocimientos tradicionales.

Decisión 391 de 1996 de la Comunidad Andina de Naciones - CAN: Es conocido como el Régimen Común de Acceso a Recursos Genéticos, en la cual se encuentra un marco regulatorio respecto del acceso a los recursos genéticos y a los conocimientos tradicionales. Donde se fijan normas sobre la propiedad intelectual dentro de la creación humana sobre los conocimientos tradicionales asociados de las comunidades indígenas, afroamericanas y otras locales constituyen su propiedad intelectual colectiva.

Decisión 291 de 1991 de la Comunidad Andina de Naciones: Contiene normas de obligatorio cumplimiento sobre la protección de la propiedad industrial para los países miembros de la CAN.

Decisión Andina 486 de 2000: Concede protección a aquellas personas titulares de derechos de propiedad industrial, estableciendo el régimen común sobre propiedad intelectual.

Sentencias

La Corte Constitucional, mediante sentencia C-276 de 1996, expresó que “el derecho de propiedad intelectual, se reconoce en cabeza de quien es creador de una obra (literaria, artística, científica, musical, teatral o audiovisual).

La Corte Constitucional, en sentencia T-367 de 2009 menciona que: “Las regalías captadas se encuentran supeditadas a la explotación que se haga de las obras musicales, pues, del impacto que tenga en el mercado en cuanto a la demanda y la adecuada gestión que se realice por la casa editora, depende en gran medida los ingresos que habrá de percibir el artista”.

La Corte Constitucional, en sentencia T-367 de 2009, indica que las creaciones del intelecto, y aquellas relacionadas con su divulgación y difusión, en cuanto bienes inmateriales han sido agrupadas, para efectos jurídicos, en los denominados derechos de propiedad intelectual, los cuales, a su vez, comprenden los derechos de autor, los derechos de propiedad industrial y los derechos sobre descubrimientos científicos, así como otras formas y manifestaciones de la capacidad creadora del individuo.

Un precedente más de la Corte Constitucional se encuentra en la sentencia C-011 de 2013, bajo el expediente D- 9107. (M. P.: Alexei Julio Estrada), en este pronunciamiento la Corte indica que la materia que regula la Ley 1520 de 2012, que es la relativa a los derechos de autor, tiene reserva de ley estatutaria por dos razones: a) en primer lugar, por cuanto la jurisprudencia de esta Corporación ha establecido que los derechos morales de autor tienen el rango de derechos fundamentales; y, b) en segundo lugar, en consideración a que varias de sus disposiciones conllevan una afectación directa de otros derechos fundamentales como la libertad de expresión y el acceso a la información, consagrados en el artículo 20 constitucional.

Solución del problema: Criterios para fomentar el respeto de las creaciones intelectuales en la industria musical relacionada con las nuevas tecnologías.

Teniendo en cuenta que la propiedad intelectual, resulta ser un producto basado en la creación de ideas innovadoras, se hace necesario establecer unos criterios que se ajusten dentro del marco normativo nacional e internacional en relación a los convenios aprobados por Colombia, Frente a lo anterior se recomienda:

Derechos editoriales: Creación de derechos editoriales, los cuales se esperan protejan la composición musical, esto a partir del establecimiento de porcentajes equitativos entre la compañía editorial y el compositor.

Derechos fonográficos: Los cuales están dirigidos a la protección de la grabación original del audio, conocida como máster. Aquí se espera que el marco legislativo establezca las tablas de cobros existentes frente a los diferentes derechos cuando la música es utilizada por otras personas.

Beneficios por los derechos de autor: Respecto de la cesión de derechos patrimoniales deberá existir unos montos o porcentajes específicos sobre la explotación económica de las obras y a cambio recibir pagos llamados regalías, las cuales son pagadas por la empresa o particular encargado de la distribución de la música, ya sea en formatos CD u otras plataformas identificadas como streaming, también se deberá establecer los costos de reproducción en radio, internet y televisión entre otros medios tecnológicos existentes actualmente. Adicional

se incluyen las regalías de música en formato impreso, lo cual exige que las partituras utilizadas por terceros den pagar una regalía para este uso.

Licencias de sampling: Las conocidas pistas, las cuales son parte integral de una obra musical, misma que en algunas oportunidades podrán ser utilizadas en la creación de otras obras, para lo cual debe existir una exigencia monetaria por dicho uso.

CONCLUSIONES.

Los derechos de autor en los sistemas musicales clásico y moderno se encuentras contenidos en diferentes normativas que han sido acogidas por los Estados entre las cuales se encuentran el Convenio de París para la Protección de la Propiedad Industrial, el Convenio de Berna para la Protección de las Obras Literarias y Artísticas de 1886, la Decisión 486 de 2000 de la Comunidad Andina de Naciones sobre el Régimen Común sobre Propiedad Industrial y el Tratado de la OMPI sobre Derecho de Autor de la Organización Mundial de la Propiedad Intelectual en el año de 1996. Así como de la Ley 33 de 1987, por medio de la cual se aprueba el Convenio de Berna para la protección de las obras literarias y artísticas, así como la Ley 23 de 1982 Sobre Derechos de Autor, entre otras que prestan protección a estos derechos.

Existe una gran amenaza para compañías editoriales y compositores, por cuanto el ordenamiento jurídico actual, resulta ser obsoleto a las nuevas exigencias de este mercado, por cuanto las nuevas tecnologías de la información y la comunicación TIC exigen de los Estados la generación de marcos normativos actualizados respecto de la protección de las obras y demás bienes inmateriales, para que así se pueda garantizar la protección de los derechos patrimoniales sin importar el soporte físico o virtual.

CAPITULO 3

DESAFIANDO LA ERA DIGITAL - UNA VISION HACIA LOS CONTRATOS DE ADHESION ELECTRONICA REDES SOCIALES.

Autores:

Jessica Andrea Basante Rosero

Luz María Molina Yela

Luisa María Navarro De Los Ríos

Cristian Alejandro Suarez Burbano

RESUMEN.

En el presente trabajo se aborda la problemática que rodea a los contratos de adhesión que se hacen de manera electrónica dentro de las redes sociales, se destaca como los usuarios en reiteradas ocasiones aceptan deliberadamente términos y condiciones dentro de éstas plataformas sin comprender completamente las implicaciones de lo que aceptan y lo que podría resultar en una vulneración de derechos así como también una invasión a la protección de datos personales. La investigación se centra en Meta (Facebook, WhatsApp, Instagram) como caso principal explorando casos en los que es evidente la falta de transparencia y el desequilibrio de poder lo cual perjudica a los usuarios. Además de esto se hace estudio de distintas normativas en Colombia y a nivel internacional (Unión Europea) y se proponen mecanismos que buscan mejorar la protección para los derechos de los usuarios destacando la realidad de la cesión de derechos que existe actualmente en el contenido creado en estas plataformas.

INTRODUCCION.

En la era digital del siglo XXI, los contratos electrónicos de adhesión se han vuelto omnipresentes, especialmente en las redes sociales, donde los usuarios a menudo aceptan los términos y condiciones sin comprender completamente sus implicaciones o tener la oportunidad de negociar; lo anterior ocasiona que en múltiples situaciones, los usuarios de las redes sociales pierdan la protección de sus datos personales ya que acceden a cláusulas que pueden tornarse en abusivas, y además de ello, quede la incógnita sobre los derechos derivados sobre la propiedad Intelectual del contenido que los mismos usuarios crean en texto, sonido, imagen o video, ya que, por falta de regulación y de conflictos jurisdiccionales, en esencia, la autonomía de la voluntad en estos contratos son los que rigen estas relaciones entre las redes sociales y sus usuarios.

El problema central abordado en esta investigación radica en los verdaderos alcances que pueden tener la protección de datos personales y los derechos de la Propiedad Intelectual, según la normatividad colombiana sobre los contratos adheridos entre los usuarios de redes sociales y éstas, teniendo como fundamento el componente de territorialidad que contiene el derecho frente a la naturaleza extraterritorial de las redes social, empleando como caso de estudio la relación entre Meta y sus usuarios en el ordenamiento interno y desde un análisis de precedentes tomados de los Estados Unidos y la Unión Europea sobre la misma problemática.

La investigación busca dar a conocer que dentro de los contratos de adhesión al suscribirse en redes sociales por ejemplo, también se está vulnerando y afectando el régimen de propiedad intelectual, de tal manera que el presente escrito intentará analizar esa dicotomía sobre los contratos de adhesión electrónica, sobre el tratamiento de los datos personales y sobre la propiedad intelectual que está involucrada al respecto, la validez de las cláusulas de renuncia de derechos y cómo se protege o debería proteger a la parte más débil en esta dinámica contractual; además, se analiza los mecanismos de resolución de conflictos en el contexto de este tipo de contratos.

Este esfuerzo propende por hacer una contribución significativa al conocimiento jurídico y social, ofreciendo análisis, discusión y recomendaciones que pueden guiar futuras reformas

legales y prácticas comerciales, por lo tanto, la investigación se presenta como un esfuerzo crucial para promover un equilibrio entre los avances tecnológicos y la protección efectiva de los derechos de los consumidores en una sociedad cada vez más digitalizada.

PLANTEAMIENTO DEL PROBLEMA.

En el siglo XXI, la era de la información y la tecnología, la contratación tradicional ha experimentado una transformación significativa con la emergencia de los contratos de adhesión electrónica, estos contratos son omnipresentes en las plataformas digitales, especialmente en redes sociales, donde los usuarios a menudo aceptan términos y condiciones sin un conocimiento pleno o una negociación de las cláusulas. La investigación se propone explorar la dicotomía entre los contratos electrónicos y la vulneración a la cual se ve sometida la propiedad intelectual , basados en la teoría de la voluntad y el acuerdo mutuo, y los contratos de adhesión electrónica, que se caracterizan por la aceptación pasiva de términos predeterminados (Hawes, 2019).

El problema radica en que la naturaleza no negociable de estos contratos plantea cuestiones legales y éticas significativas, particularmente en lo que respecta a la privacidad, la protección de datos personales y la cesión de derechos; a pesar de que la legislación busca proteger la intimidad y la dignidad de los individuos, las redes sociales utilizan información personal, creaciones literarias, artísticas y científicas sin el consentimiento explícito de los usuarios, lo que plantea interrogantes sobre la vulneración de los derechos fundamentales y la paternidad del autor sobre sus creaciones.

La investigación abordará el conocimiento y la comprensión del consumidor promedio frente a la sesión del tratamiento de los datos personales y la protección de sus derechos en el marco de la propiedad intelectual, la validez de las cláusulas de renuncia de derechos, especialmente el derecho a litigar en tribunales, y cómo se protege o se debería proteger a la parte más débil en esta dinámica contractual; además, se analizará los mecanismos de resolución de conflictos en el contexto de los contratos de adhesión electrónica.

HIPOTESIS.

La hipótesis planteada es: "Los contratos de adhesión electrónica en redes sociales, como los implementados por Meta, contribuyen a una desigualdad contractual y a la vulneración de los derechos de privacidad de los usuarios debido a la falta de transparencia y al desequilibrio en el poder de negociación, lo que lleva a una aceptación pasiva de términos y condiciones que no se entenderían ni se aceptarían en un entorno de contratación tradicional, cediendo en su totalidad la información y uso de imágenes, videos y cualquier tipo de contenido que se agregue a este tipo de plataformas, para que sean ellas quienes comercialicen, usen y distribuyan los datos de los consumidores sin solicitar ningún permiso a los suscriptores."

Esta hipótesis se basa en la premisa de que la naturaleza "tomar o dejar" de esta clase de contratos, la complejidad de los términos coloca a los usuarios en una posición desventajosa y a menudo llevan a una erosión de sus derechos legales y personales, limitando la creatividad de los usuarios ya que pueden verse limitados en su capacidad para usar contenido protegido por derechos de autor, incluso para fines no comerciales como la crítica, el comentario o la parodia.

JUSTIFICACION.

La investigación se justifica en el contexto de una era digital en constante evolución, donde las plataformas digitales y las redes sociales han transformado no solo nuestras interacciones sociales, sino también las transacciones comerciales y las relaciones legales; esta transformación ha dado lugar a la proliferación de contratos de adhesión electrónica, donde los términos y condiciones se aceptan sin una negociación previa, planteando interrogantes sobre la voluntad real, el consentimiento informado de los usuarios y la vulneración de los derechos de propiedad intelectual. La relevancia radica en la creciente preocupación por la privacidad de los datos y la protección de los derechos personales en el vasto marco de la información digital, a medida que las plataformas como Meta se convierten en centros

omnipresentes para la interacción social, la cesión de derechos y el uso de información personal por parte de terceros generan profundas implicaciones éticas y legales (Burneo & Antonio, 2008)

Esta investigación también busca explorar la efectividad de los mecanismos de solución de disputas actuales, como los tribunales de arbitraje, y la adecuación del marco legal ante los desafíos presentados por los contratos de adhesión electrónica, la necesidad de evaluar si estos sistemas proporcionan una protección suficiente a la parte más débil subraya la importancia de reconsiderar y fortalecer estos mecanismos para asegurar la equidad y la justicia en el entorno digital (Keymer & Troxler, 2008); al profundizar en estas cuestiones, el estudio promete aportar una contribución significativa al conocimiento jurídico y social, ofreciendo análisis, discusión y recomendaciones que puedan guiar futuras reformas legales y prácticas comerciales. De este modo, la investigación se presenta como un esfuerzo crucial para promover un equilibrio entre los avances tecnológicos y la protección efectiva de los derechos de los consumidores en una sociedad cada vez más digitalizada.

MARCO DE REFERENCIA.

La emergencia de los contratos electrónicos representa un cambio significativo hacia métodos más rápidos y eficientes, facilitados por la tecnología digital, los contratos electrónicos se crean, firman y almacenan digitalmente, permitiendo a las partes realizar acuerdos a distancia sin necesidad de encuentros presenciales o documentos físicos; la aceptación de estos contratos está respaldada por leyes que reconocen su validez, como el Acta de Firmas Electrónicas en Comercio Global y Nacional (E-Sign Act) en EE. UU. y la Acta de Comunicaciones Electrónicas en el Reino Unido, asegurando que un acuerdo o transacción no se invalide simplemente por ser electrónico (Rodríguez, 2004).

La diferencia clave entre los contratos tradicionales y los electrónicos radica en su formato y proceso de formalización, mientras que los contratos tradicionales requieren una serie de pasos meticulosos que pueden ser tiempo consumiendo, los contratos electrónicos ofrecen una eficiencia notable al reducir el tiempo de respuesta, resistir el fraude y la manipulación

mediante medidas de seguridad como la verificación de OTP (contraseña de un solo uso) y certificados digitales, y disminuir los costos de gestión y almacenamiento al eliminar la necesidad de espacios físicos para su archivo. En el contexto de la nueva era digital, particularmente en plataformas digitales y redes sociales, los contratos electrónicos ofrecen la flexibilidad de integrarse con activos y servicios digitales, promoviendo una adaptabilidad al paisaje digital en constante evolución; además, contribuyen a un impacto ambiental reducido al eliminar la necesidad de imprimir, servicios postales o archivado físico, lo que los convierte en una opción más sostenible y eco-amigable para las transacciones comerciales A medida que la tecnología continúa avanzando, es probable que el uso de contratos electrónicos aumente, ofreciendo una conveniencia, seguridad y eficiencia mejoradas; sin embargo, es crucial estar informado sobre el panorama legal y los requisitos específicos de la jurisdicción al elegir el tipo de contrato adecuado para necesidades comerciales o personales (López, 2012).

PROTECCION DE LA INTIMIDAD Y LA DIGNIDAD EN CONTRATOS ELECTRONICOS EN EL CONTEXTO COLOMBIANO

En el contexto colombiano, los contratos de adhesión electrónica, especialmente en plataformas de redes sociales como Meta, presentan desafíos legales y doctrinales significativos; un aspecto destacado es la gestión de los datos personales de los usuarios por parte de estas plataformas, la discusión se centra en si la autorización para el tratamiento de datos personales por parte del usuario, necesaria para utilizar servicios como Facebook, puede considerarse una contraprestación onerosa, lo que convertiría estos acuerdos en contratos de suministro de servicios; aunque los datos personales por sí mismos no tienen valor monetario, su agregación y análisis sí pueden generar beneficios económicos significativos para las plataformas, sugiriendo que hay una contraprestación por parte del usuario (Moreno, 2021).

METODOLOGIA.

La metodología de este estudio se basa en una revisión exhaustiva de la literatura existente sobre contratos de adhesión electrónica en redes sociales y en especial en el análisis de las cláusulas que se puedan considerar abusivas respecto de la protección de datos personales y

de los derechos de Propiedad Intelectual sobre las creaciones de texto, imagen, sonido y videos en redes sociales. Se llevará a cabo una revisión de fuentes secundarias, que incluye investigaciones académicas, jurisprudencia, regulaciones legales y doctrina relevante en el contexto colombiano y global; además, se realizará un análisis comparativo frente a la protección de los derechos de los usuarios frente a estos componentes abusivos de Meta, como caso de estudio de redes sociales, basados no solo en la teoría de la autonomía de la voluntad, sino también, en la realidad de contexto frente al usuario y a la aplicación normativa y jurisdiccional que se ha adelantado en otros ordenamientos, especialmente Estados Unidos y la Unión Europea. Esto permitirá identificar las diferencias fundamentales y las implicaciones legales; en este sentido se empleará como técnica de recolección de información la revisión bibliográfica bajo un enfoque cualitativo.

EL USO DE DATOS PERSONALES EN LAS REDES DE META.

Como ya se ha indicado, la relación existente entre las diferentes redes sociales y sus usuarios es por excelencia una relación de adhesión, en la que, quien pretenda ser usuario solo tiene dos posibilidades, o aceptar las diferentes políticas indicadas en las redes sociales, o abstenerse de acceder a estas. De hecho, al ingresar y crear un usuario, lo que hace cada persona de manera intrínseca es aceptar dichas políticas, o lo que, para efectos de consecuencias jurídicas, se puede denominar, suscribir el contrato de adhesión.

Se analiza directamente lo que sucede respecto de los datos personales en las aplicaciones que corresponden a Meta Platforms Ireland[14], es decir, Facebook, Instagram y WhatsApp, pero que se extiende a todos los productos que tiene Meta, que son las app Boomerang y Threads, productos de Facebook Portal, Meta Horizon Worlds, Meta Quest, Tiendas, Marketplace, Spar AR, Herramientas empresariales de Meta, Meta Audience Network, Facebook View, Meta Pay y experiencias de finalización de compra de Meta, según queda establecido por Meta (2024)

[14] Se ha podido identificar que ya existe un antecedente de Investigación que analiza el tratamiento de los datos personales en el caso Meta, realizado en 2023 en España por Sánchez Rodríguez, Raquel, y que aborda la sanción de la UE a Meta por infracción a los derechos derivados del uso de datos personales, pero el mismo no se encuentra disponible para consulta, por lo que no puede considerarse en la citación de este documento. Su información se encuentra en https://dialnet.unirioja.es/servlet/articulo?codigo=9156204

De hecho, estos productos que habitualmente el usuario de redes sociales desconoce o usa considerando que hacen parte de la misma red social, como puede suceder con Marketplace en Facebook, por ejemplo, tienen políticas de privacidad complementarias, según advierte Meta (2024). Esto puede ocasionar mayores riesgos sobre los derechos del hábeas data sobre los usuarios. Se puede pensar por ejemplo en una persona que no usa estas plataformas sociales, pero que quiere vender un producto, por lo que abre una cuenta en Facebook exclusivamente para realizar dicha venta en Marketplace, sin saber que al hacerlo, está entregando toda su información personal a más de 15 productos diferentes que hacen parte de la plataforma Meta y no solo esto, "Para ilustrar la magnitud de este fenómeno, sepa el lector que en tan solo sesenta segundos se comparten 65.000 fotos en Instagram, 167 millones de videos son vistos en Tiktok, se accede a 694.000 videos desde YouTube y se escriben 575.000 tuits" (Morán, 2022).

Aunado a lo anterior, otro interrogante surge en medio de las dudas que genera el uso del tratamiento de datos personales a través de Meta, y es que existen millones de usuarios que ingresaron y crearon sus cuentas en Facebook desde sus orígenes en 2004[15] bajo unos lineamientos de protección de datos específicos sobre lo que se publicaba en esta red social, lo que no incluía a los otros 16 productos que hoy hacen parte de Meta y que fueron ingresando poco a poco, por lo que unilateralmente Facebook y posteriormente Meta fueron modificando las políticas del uso y tratamiento de datos personales a sus usuarios para incorporar estos nuevos productos, es de vital importancia para el desarrollo de la presente investigación dar a conocer la cláusula de términos y condiciones referente al tratamiento de datos personales y la propiedad intelectual en general que vincula a los suscriptores directamente con Meta y las diferentes redes sociales. "Eres el propietario de los derechos de propiedad intelectual (como derechos de autor o marcas comerciales) de todo el contenido que crees y compartas en Facebook y en los demás Productos de las empresas de Meta que uses. Ninguna disposición en estas Condiciones anula los derechos que tienes sobre tu propio contenido. Puedes compartir libremente tu contenido con quien quieras y donde quieras.

15 De acuerdo con la información publicada oficialmente por Meta en su página, el lanzamiento de Facebook fue en este año, específicamente el 4 de febrero de 2004.

Sin embargo, para proporcionar nuestros servicios, necesitamos que nos otorgues algunos permisos legales (conocidos como "licencias") para usar este contenido. Esto es exclusivamente para proporcionar y mejorar nuestros Productos y servicios, como se describe en la sección 1 anterior.

En concreto, cuando compartes, publícas o subes contenido que se encuentra protegido por derechos de propiedad intelectual en nuestros Productos, o en relación con ellos, nos otorgas una licencia internacional, libre de regalías, sublicenciable, transferible y no exclusiva para alojar, usar, distribuir, modificar, publicar, copiar, mostrar o exhibir públicamente y traducir tu contenido, así como para crear trabajos derivados de él (de conformidad con tu configuración de privacidad y de la app). Esto significa, por ejemplo, que, si compartes una foto en Facebook, nos concedes permiso para almacenarla, copiarla y compartirla con otros (por supuesto, de conformidad con tu configuración), como proveedores de servicios o Productos de Meta que respaldan esos servicios y productos. La licencia finalizará una vez que se elimine tu contenido de nuestros sistemas.

Puedes eliminar el contenido individual que compartes, publicas o subes cuando quieras. Asimismo, si eliminas tu cuenta, se eliminará también todo el contenido que hayas publicado en tu cuenta personal. Obtén más información sobre cómo eliminar tu cuenta. Si eliminas tu cuenta, no se elimina automáticamente el contenido que publicas como administrador de una página ni el que creas en colaboración con otros usuarios, como las fotos de los álbumes compartidos que seguirán siendo visibles para el resto de los miembros." (Meta. 2024) es de menester importancia reconocer que el consumidor promedio no entiende, ni tampoco lee los términos y condiciones implícitos en las plataformas.

Esto tiene sentido si se considera que Facebook fue lanzado en 2004, Messenger inició el 9 de agosto de 2011, Instagram fue adquirido el 9 de abril de 2012, WhatsApp el 19 de febrero de 2014, Oculus el 25 de marzo de 2014 y Meta finalmente fue creado el 28 de octubre de 2021. (Meta, 2024, s.p.) Es decir, que antes de la existencia de Meta y con ello las actuales políticas comunes a los diferentes productos que hacen parte de esta marca empresarial, había usuarios de hasta 17 años de antigüedad que pudieron seguir empleando sus redes sociales sin darse cuenta de lo que significaba para su protección de datos personales la unificación de todos estos productos, aun cuando solo use uno de ellos.

Respecto a esta política de uso de datos personales actual y general para todos los productos de Meta, se destacan, entre otros algunos elementos, el primero, el tipo de información que Meta recopila, esto es, la información al momento de registrarse, lo que el usuario hace a través de sus productos, los amigos o seguidores, la información del teléfono, computador, tableta o cualquier dispositivo en el que se usen dichos productos y la información que se toma de estos dispositivos sobre lo que se hace por fuera de los productos de Meta. (Meta, 2024, s.p.)

Lo anterior es una aceptación para que Meta conozca dentro de los navegadores de Internet a qué información se está accediendo, lo que podría ser delicado si se pretende proteger la información personal de cada persona en internet. Delicado lo es también la recopilación de datos que hace Meta aun cuando no se tiene una cuenta, pero se usan los productos de Meta, en donde se recopila información como los registros de los navegadores, las apps que se visitan, en donde como lo expone la misma empresa, "Por ejemplo, también puedes ver anuncios de los Productos de las empresas de Meta por medio de Meta Audience Network cuando visitas otras apps si no podemos reconocerte como usuario registrado de los Productos de Meta." (Meta, 2024, s.p.)

Es por ello, que aun, sin ser usuario registrado en ninguna de las aplicaciones de Meta que, cada persona recibe publicidad en sus dispositivos electrónicos sobre bienes y servicios que el algoritmo de Meta considera que son acordes con el usuario del computador o celular, aunque no se haya registrado en ninguna red social. A esto, se suma que, a diferencia de lo que sucede con la protección de datos personales en la ley 1581 (2012), que prohíbe que la información personal que contenga una empresa sobre cada persona pueda ser compartida con terceros, en Meta por ejemplo, al acceder y registrarse, se está otorgando el consentimiento para que se entregue cualquier información personal a anunciantes que muestran anuncios en las aplicaciones de Meta, a empresas que comercializan productos de Meta, a empresas encuestadoras y de atención al cliente y a investigadores, según las Políticas de Privacidad del conglomerado de plataformas Meta (2024). No obstante, Meta no advierte por ejemplo a qué clase de investigadores se refiere, ni cómo filtra la información para determinar si quien requiere de la información de sus usuarios tiene o no las calidades indicadas en sus políticas de datos personales.

Podría preguntarse si la Ley 1581 (2012) es una norma imperativa sobre la que no se pueda pactar en contrario, o si, por el contrario, es una norma sobre la que puede prevalecer la autonomía de la voluntad, ya que pueden suceder dos escenarios diferentes. Si el primer escenario es cierto, es decir, la norma tiene contenido imperativo, entonces se puede deducir que la cláusula que permite que los datos personales se compartan indiscriminadamente con terceros para el caso colombiano sería nula. Si por el contrario, lo cierto es el segundo escenario, en donde la autonomía de la voluntad puede prevalecer, entonces esto quiere decir, que cualquier empresa, vía adhesión puede establecer cláusulas que le sean flexibles para compartir los datos personales con terceros, afectando los datos personales de los usuarios y dejando sin efectos la normatividad aplicable en la actualidad en el ordenamiento interno, máxime tratándose de la transferencia de datos a terceros países, lo cual se encuentra plenamente prohibido en la Ley 1581 (2012).

Lo cierto es que la norma de manera expresa no indica que no se pueda pactar en contrario, y ante el silencio del legislador en los últimos años en los que ha avanzado sobremanera la evolución de las redes sociales y su uso, todo parece indicar que se está en presencia de relaciones exclusivamente privadas, entre el usuario y la red social, lo cual, de ser así, y amparado en las fuentes de las obligaciones en materia comercial, si tendrá prelación las estipulaciones contractuales, aun cuando estas no estén sometidas a negociación como ocurre con los contratos de adhesión.

Sin embargo, esta problemática que enfrenta hoy el ordenamiento jurídico interno ya ha sido dirimida en otras normatividades, específicamente en la Unión Europea con la Directiva 2011/83/UE sobre los derechos de los consumidores, donde sustituyó y modificó antiguas directivas. En esta directiva incorpora con mayor fuerza los derechos de los consumidores estableciendo normas relativas al suministro de información, los derechos de desistimiento y las obligaciones contractuales. Con lo anterior se puede expresar que Meta se ha visto sujeto a diferentes resoluciones administrativas y judiciales a causa de incumplimiento a la protección de datos personales de la población de la Unión Europea.

Entre dichas resoluciones, se destaca que para enero de 2023 Meta fue multado primero con 390 millones de euros por Facebook e Instagram y luego con 5,5 millones de euros por WhatsApp por incumplir el reglamento de protección de datos personales de la Unión

Europea, todo bajo el presupuesto que los cambios se realizaban "con fines de mejora y seguridad del servicio" según reportó El Espectador (2023) y sin que sean las primeras sanciones económicas a las que fue sometido Meta por los mismos conceptos.

Pese a lo anterior, en la Unión Europea se ha ido más allá, toda vez que el Tribunal de Justicia de la Unión Europea (2023) en sentencia del asunto C 252 de 2021 indicó que Meta respecto de las políticas de uso de datos personales ha incurrido en abuso de la posición dominante en el contrato con sus usuarios, en el abuso consistente en el tratamiento de datos personales de sus usuarios y en ilicitud del tratamiento de datos personales, ya que para el Tribunal Europeo no es suficiente que dentro del clausulado del uso de las redes sociales se encuentre establecido la transferencia de datos personales a terceros, sino que, en su consideración, cada usuario debe tener la posibilidad de otorgar o no su consentimiento expreso e informado, donde cada uno indique si autoriza o no a Meta para que pueda usar sus datos personales con fines de anuncios.

En Colombia por su parte, también han existido conflictos respecto al uso de los datos personales por parte de las redes sociales, pero de una manera distinta. Para el caso colombiano, a través de vía tutela, los accionantes han buscado la protección de derechos fundamentales de la intimidad o la libertad de expresión por medio de las redes sociales, pero donde han accionado frente a terceros, y no frente a la red social o a las políticas de tratamiento de datos personales, por lo que jurisprudencialmente no existe para el caso colombiano, precedente que permita establecer si el consentimiento al momento de registrarse en la red social, o en Meta, como es el caso de estudio, es suficiente para autorizar a dicha plataforma y a sus productos para usar y compartir los datos personales.

Con motivo de este documento se han analizado las sentencias de la Corte Constitucional SU 420 de 2019, T 280 de 2022, T 339 de 2022 y T 241 de 2023, encontrando como elemento común en todas ellas que se trata, en efecto de una protección sobre derechos fundamentales, no solo los indicados de libertad de expresión e intimidad, sino también de la honra y buen nombre derivados de las publicaciones realizadas por particulares en redes sociales, pero sin llegar a la discusión que se ha planteado en este capítulo. Se torna relevante y pertinente que se estudie si en efecto, tal como sucedió con la Unión Europea y con motivo de dar cumplimiento a la normatividad vigente en la actualidad, debería limitarse la expresión de la

voluntad al registrarse en la red social, y de imponerse la carga a Meta de elaborar un consentimiento informado, claro, expreso e inequívoco del uso y transferencia de datos personales de los usuarios en territorio colombiano de sus productos para evitar la laguna frente a la ley de hábeas data que hoy se encuentra configurada, ya que, como se encuentran las cosas, Meta tiene en el ordenamiento interno el monopolio para transferir los datos personales de sus usuarios.

En el contexto colombiano no existe una regulación específica para contratos electrónicos, en el mejor de los casos aplican la ley 1480 del 2011, es también conocida como el Estatuto del Consumidor y tiene como objetivo principal proteger, promover y garantizar la efectividad y el libre ejercicio de los derechos de los consumidores, sin embargo, no da un estudio profundo de cómo garantizar la protección de los derechos de usuarios dentro de los contratos de adhesión, por el contrario gracias a la investigación del blog de CEDRO nos informa que en el ordenamiento jurídico de España en su Decreto Legislativo 1/1996 de 12 de abril, por el que se aprueba el texto refundido de la ley de propiedad intelectual (TRLPI) recoge una lista cerrada de límites y excepciones de los derechos de propiedad intelectual. En su artículo 100 encontramos los límites a los derechos de explotación relativos a programas de ordenador y en el 135 están los aplicables al derecho sui generis del fabricante de base de datos estos han sido complementados gracias al Real Decreto-Ley 24/2021, de 2 de noviembre.

En estas complementaciones en el mismo canal informativo el blog de CEDRO se vislumbra la autorización para usuarios determinados que quieran abordar unos usos concretos, estos tienen que cumplir con una serie de requisitos o condiciones que se encuentran impuestos en el límite del mismo. Solo el receptor de cada límite podrá ser el beneficiario del trabajo en cuestión y solo estos exclusivamente tendrán el derecho autorizado de realizar actos como reproducción, distribución, comunicación pública o transformación, si se realizan diferentes actos que no estén cubiertos por el límite, obligatoriamente deben ser autorizados por los titulares de derechos. De esta manera si el beneficiario de un determinado límite que por ejemplo sólo permite realizar la reproducción de la obra únicamente tiene la facultad de hacer el acto de copia de misma en condiciones anteriormente establecidas, pero no se tendrá permitido realizar la explotación de esta, como distribución.

Por otro lado en la legislación argentina se puede ver regulado los contratos de adhesión en su Código Civil y Comercial Aprobado por ley 26.994, Promulgado según decreto 1795/2014, Actualizado con las modificaciones introducidas por las leyes 27.551, 27.586 y 27.587, al igual que la ley de defensa del consumidor. Con se busca que las normas reguladoras sobre las mismas cosas, estén dentro de un mismo ordenamiento jurídico, con esto se pretende que ninguna norma derogue a la otra. Se puede inferir que a pesar de que esta situación no es común, obliga a una buena y necesaria convivencia, así como la complementación entre ambos cuerpos normativos. Como en el caso de los contratos de adhesión.

Según un estudio realizado por FERNANDO E. SHINA para la SAIJ (Sistema Argentino de Información Jurídica).

> En la sistemática del CCyC, los contratos de adhesión, que en rigor se denominan Contratos celebrados por adhesión a cláusulas generales predispuestas, fueron ubicados en el Libro III, Título II, Capítulo 3, Sección 2, arts. 984 a 989 inclusive. Es decir, forman parte de los contratos paritarios, cuyo tratamiento, dentro de ese mismo Título II, comienza en el art. 957.
>
> Esta cuestión, que es puramente sistemática, no es, sin embargo, de menor importancia. Por el contrario, esa ubicación metodológica dispone que los contratos de adhesión (en adelante CA) sean un subgrupo dentro de los contratos clásicos.
>
> Según nuestra opinión, esta clasificación que les niega autonomía a los contratos de adhesión es un error sistemático porque, como veremos, más allá de su ubicación en el CCyC, los contratos de adhesión no se rigen por los mismos principios y las mismas reglas que regulan a los contratos paritarios.

LA CESION DE DERECHOS Y LA PROPIEDAD INTELECTUAL SOBRE LAS PUBLICACIONES.

Según Meta (2024),

> Es posible que se apliquen otras condiciones y políticas cuando utilices las herramientas empresariales de Meta en conjunto con las Condiciones de la plataforma o las Condiciones de anuncios de autoservicio, u otros productos específicos de publicidad o medición.
>
> Además, en función de los productos o servicios que se utilicen, también se aplicarán políticas y condiciones de uso generales. Estas incluyen, entre otras, las Condiciones del servicio, la Política de privacidad, las Condiciones comerciales, las Normas de publicidad, las Políticas de páginas, grupos y eventos y las Condiciones de uso de Instagram. (s.p.).

Al observar las Condiciones del servicio, la Política de privacidad, las Condiciones comerciales, las Normas de publicidad, las Políticas de páginas, grupos y eventos y las Condiciones de uso de Instagram, se encuentra que todo usuario otorga algunos permisos por usar los productos de Meta y que son en esencia, el permiso para usar contenido creado y compartido, a lo que Meta denomina "licencias" (Meta, 2024, s.p.), lo cual, en teoría se especifica desde la concepción que quien crea la publicación, tratándose de texto, imágenes o videos, es el titular de los derechos de Propiedad Intelectual que se puedan derivar de esta, atendiendo a los derechos morales y a los derechos patrimoniales sobre la obra objeto de protección, pero dentro de un régimen especial que se hace necesario establecer.

Por una parte, la Decisión Andina (1993) que es la norma regional que establece la protección de los derechos de autor y que es vigente y vinculante vía Bloque de Constitucionalidad en el estado colombiano, establece que los derechos de autor pueden ser de autor o derechos conexos, que se pueden catalogar de la siguiente manera:

Derechos de Autor[16]: Los derechos de autor son un conjunto de derechos exclusivos concedidos a los creadores de obras originales o sus representantes legales. Estos derechos protegen la expresión de ideas y la creatividad en diversas formas, como libros, música, obras

[16] La información contenida sobre los conceptos de Derechos de Autor y derechos conexos es de creación propia, pero con base en lo descrito en la Decisión Andina.

de arte, películas, software y otras obras intelectuales y hacen parte de los derechos de la propiedad intelectual.

Derechos conexos: Los derechos conexos a los derechos de autor se refieren a un conjunto de derechos que protegen a las personas y entidades que participan en la creación y difusión de obras, pero que no son los creadores originales. Estos derechos protegen a intérpretes, ejecutantes, productores de fonogramas y organismos de radiodifusión en relación con sus contribuciones y actividades.

Atendiendo estos conceptos, se podría indicar que la creación de texto, imagen, sonido o video que se pueda subir y compartir a través de las redes sociales y productos de Meta corresponde a quien lo creó, y que Meta por su parte, en calidad de medio por el que se realiza la difusión, puede ser titular de derechos conexos. Sin embargo, debido a la autonomía de la voluntad descrita en el vínculo jurídico entre Meta y sus usuarios, lo cierto es que ocurre otra cosa.

De acuerdo con las condiciones generales de Meta (2024), si bien, el creador es titular de los derechos de autor sobre sus creaciones, a diferencia de lo que puede suceder con otro tipo de obras protegidas, el creador no cuenta con la disponibilidad de vender su contenido creado y disponer patrimonialmente de éste, sino que sus derechos de creación están relacionados específicamente con los derechos morales; esto, ya que Meta se reserva varios permisos o licencias que le conceden sus usuarios.

Por una parte, el usuario creador de texto, imagen, sonido o video está concediendo permiso para que Meta almacene, copie y comparta dicha publicación, permiso que sucede incluso después de que la publicación original haya sido eliminada, debido a que Meta se reserva entre 30 y 90 días con el contenido, incluso aunque no sea visible para los usuarios ni para el creador.

Aunado a lo anterior, si Meta considera que el contenido era violatorio de sus políticas, se reserva la posibilidad de apropiarse de ese contenido por un período mayor, lo que quiere decir que, aunque en teoría el creador sea titular de derechos de autor, en esencia, el aspecto patrimonial ha sido cedido intrínsecamente a Meta.

Esta situación se puede acentuar, si el contenido que se publica llega a tener cualquier imagen o símbolo que identifique a cualquier producto de Meta. Como lo indica Meta (2024),

> Si usas contenido protegido por derechos de propiedad intelectual que poseemos y ponemos a disposición en nuestros Productos, tales como imágenes, diseños, videos o sonidos que ofrecemos y que tú agregas al contenido que creas o compartes en Facebook, nos reservamos todos los derechos sobre dicho contenido (pero no sobre los tuyos). Solo puedes usar nuestros derechos de autor o nuestras marcas comerciales o cualquier marca similar según lo permiten nuestras Normas de uso de marca de forma expresa o con nuestro permiso previo por escrito. Debes obtener nuestro permiso por escrito (o contar con uno en virtud de una licencia de código abierto) para modificar, traducir o descompilar nuestros productos o sus componentes, así como para aplicar ingeniería inversa o crear obras derivadas de ellos, o para intentar extraer de algún otro modo el código fuente, salvo excepciones o limitaciones en virtud de la ley aplicable o si realizas estas acciones en relación con el Programa de recompensas por reporte de errores de Meta. (n. 4)

En otros términos, cualquier creación en la que se incluya algún signo distintivo, debido al contrato suscrito, tiene Propiedad Intelectual respecto a los derechos de autor y a los derechos de la Propiedad Industrial exclusivamente en favor de Meta, o lo que es lo mismo, el usuario renuncia de manera tácita a cualquier propiedad sobre dicha creación, en este caso incluyendo a los derechos morales.

Nuevamente se está frente a una vulneración de la normatividad vigente en Colombia, ya que, en el ordenamiento interno los derechos de propiedad industrial y de derechos de autor se encuentran regulados a partir de la Decisión Andina (1993) y la Decisión Andina (2000) e incluyen protección a ambos derechos derivados de la Propiedad Intelectual en el sentido que, para el caso de los derechos de Propiedad Industrial debe existir registro ante la Superintendencia de Industria y Comercio y en el caso de los derechos de autor, los derechos pertenecen a quien crea, como en este caso, la publicación en texto, imagen, sonido o video.

Sin embargo, y frente a una normatividad general y que no se ha preparado para enfrentar los desafíos que llegan con el auge de las redes sociales y de la extraterritorialidad que ellas representan, Meta ha logrado apropiarse de derechos de propiedad intelectual, que, en esencia, por regulación expresa, no le corresponden.

Es así como se puede observar, por ejemplo, en Instagram o en Facebook, o incluso en los recién creados canales de WhatsApp, que existen creadores de contenido que se dedican a la creación de videos, y de los cuales, reciben simplemente en aporte una parte de lo que por concepto de publicidad recibe Meta de la publicidad que se cuelga en dichas publicaciones. La regulación en el caso colombiano frente a esta realidad es inexistente y, por tanto, los creadores de contenido en estos casos aceptan de manera tácita el monto que Meta decide unilateralmente que pagará en favor del creador, toda vez que la explotación de los derechos patrimoniales está en cabeza de este conglomerado de plataformas y productos, y el creador es visto solo como un canal por medio del cual se llega al público objetivo de las empresas que pagan los anuncios que se publicitan.

Esta afirmación es tan cierta, que encuentra asiento en varios aspectos, el primero, que Meta pueda seguir disponiendo de las publicaciones, aun cuando el creador decida eliminar la publicación, e incluso, eliminar la cuenta; el segundo, porque Meta tiene la facultad de suspender o cancelar unilateralmente las publicaciones o cuentas a su libre arbitrio, lo que demuestra que es el propietario de las publicaciones y no el usuario, y además de ello, no permita ningún debido proceso para que el usuario pueda recurrir a dicha decisión unilateral.

Finalmente, otro vacío que se encuentra frente a la Propiedad Intelectual surge respecto de las cuentas y publicaciones que continúan online cuando la persona fallece, ya que, si bien, Meta (2024) ha implementado el contacto de legado, se debe verificar el verdadero alcance que se está dando a esta figura, o si simplemente ha quedado en la política de Meta, pero sin extenderse en verdad a la realidad, y frente a lo que pueden existir otras víctimas distintas de la persona fallecida.

Ejemplo de ello, son los videos que se publican sobre homicidios. Es común que se publiquen los videos de las cámaras de seguridad en donde se ve que alguien es asesinado y a su lado, una fotografía en vida y algún texto que lo identifique. En esos casos, el dolor de la familia,

de sus hijos, cónyuge y padre, entre otros, encuentra una revictimización al poner en la palestra pública a su familiar fallecido tanto en texto, como en imagen y video, y en donde Meta al parecer, no se hace responsable, basado en sus políticas internas.

Frente a estas situaciones, se encuentran también los derechos de los niños, niñas y adolescentes que tienen una especial protección constitucional conforme a los artículos 42 y siguientes de la Constitución Política (1991). Frente a ellos, aunque Meta en sus políticas establece como edad mínima para ser usuario de sus productos los trece (13) años de edad, lo cierto es que existen menores de esa edad como usuarios, ya que no hay filtros que permitan frenar el ingreso de población menor a las redes sociales.

Sobre este punto, en Estados Unidos se denunció a Meta por ser directo responsable de autolesiones y suicidios de niños, niñas y adolescentes, a lo que, por primera vez, el creador de Facebook y CEO de Meta, Mark Zuckerberg, pidió perdón por los daños generados por las redes sociales, el pasado primero de febrero (BBC, 2024, s.p.). en este escenario, frente al Congreso de los Estados Unidos, se pudo evidenciar que en Instagram, por ejemplo, existen videos de abuso sexual infantil, y que lo único que hace la red, como propietaria de los derechos de la propiedad intelectual, en lugar de eliminar la publicación y ponerla al conocimiento de la autoridad competente, es mostrarla oculta con la advertencia que se puede estar a punto de ver material de abuso sexual infantil, preguntando al usuario si le gustaría "ver los resultados de todos modos", según reportó BBC (2024).

Con todo esto, puede notarse no solo la problemática que se esté en manos de Meta como propietario de los derechos a la propiedad intelectual contrariando las normas vigentes en el ordenamiento interno, sino que además, se vulneren los derechos de las personas fallecidas y sus familiares, e incluso que se publiquen en sus redes abiertamente contenido ilegal, todo esto, bajo la premisa de la explotación patrimonial de todo el contenido que se sube en sus redes y productos, y del cual, por disposición propia y unilateral, el propietario de los derechos de propiedad intelectual, es Meta.

LOS MECANISMOS DE PROTECCION EXISTENTES.

Observados todos los desafíos que se han identificado en los dos capítulos anteriores, respecto del uso de datos personales y su protección, así como de la Propiedad intelectual por las creaciones en redes sociales y de la protección de las personas frente al contenido publicado, cuando se trata de personas fallecidas y de niños, niñas y adolescentes, aclarando que son solo algunas de las problemáticas a las que se enfrenta el contenido en Meta, surge el interrogante sobre cuál es el mecanismo idóneo para proteger los datos personales, la propiedad intelectual y a las personas por las publicaciones en Meta, especialmente al tener en cuenta el carácter de territorialidad que contiene el derecho, y el componente internacional de Meta.

Frente a ello, Meta (2024) establece que,

> Si eres consumidor, las leyes del país donde resides se aplicarán a cualquier demanda, acción o disputa que presentes contra nosotros y que surja como consecuencia de estas Condiciones o los Productos de Meta, o en relación con ellos. Asimismo, puedes resolver la demanda en cualquier tribunal competente de dicho país que tenga jurisdicción. En el resto de los casos, y para cualquier demanda, acción o disputa que Meta inicie contra ti, Meta y tú aceptan que se debe resolver exclusivamente en el Tribunal de Distrito de los Estados Unidos para el Distrito Norte de California o en un tribunal estatal ubicado en el condado de San Mateo. Asimismo, aceptas someterte a la jurisdicción de cualquiera de estos tribunales con el propósito de litigar cualquier demanda, y aceptas que estas Condiciones y cualquier otra demanda, acción o disputa se regirán por las leyes del estado de California, independientemente de cualquier disposición sobre conflicto de leyes. Sin perjuicio de lo anterior, aceptas que Meta, a su exclusivo criterio, puede presentar cualquier demanda, acción o disputa que tengamos en tu contra ante cualquier tribunal competente en el país en el que residas y que tenga jurisdicción sobre la demanda. (n. 4)

Lo anterior permite establecer que para el caso de las disputas que puedan surgir con usuarios en Colombia, sí tiene competencia la jurisdicción colombiana y frente a normatividad propia.

Sin embargo, tal como ha sucedido en Estados Unidos y en la Unión Europea, para que se subsanen los conflictos y problemáticas identificados, se requiere que los usuarios acudan a la jurisdicción y ventilen el conflicto, ya que, por ser derivado de una relación contractual, no se puede iniciar de oficio. Adicionalmente, por tratarse de contratos de adhesión, y de no existir cláusula compromisoria, la competencia no está delegada a Tribunales de Arbitramento, e incluso, al existir, por Estatuto del Consumidor, dicha cláusula no tiene efectos jurídicos.

¿SE VULNERAN LOS DERECHOS DE AUTOR AL ACEPTAR LAS POLITICAS DE PRIVACIDAD DE META?

En la era digital, las aplicaciones móviles como Meta se han convertido en herramientas omnipresentes en la vida diaria. Sin embargo, la descarga y uso de estas plataformas implica la aceptación de sus políticas de privacidad, las cuales generan controversia en torno a la posible vulneración de los derechos de autor y la propiedad intelectual.

Los derechos de autor protegen las obras originales de la mente humana, como textos, imágenes y videos. En el ámbito digital, la propiedad intelectual cobra especial relevancia debido a la facilidad de reproducción y distribución de contenido.

Las políticas de privacidad de Meta, al ser contratos de adhesión, no admiten negociación y obligan al usuario a aceptarlas para acceder a la plataforma.

Las políticas de privacidad de Meta establecen que:

Los usuarios conceden a Meta una licencia no exclusiva, gratuita, transferible y sublicenciable para usar, reproducir, distribuir, modificar, traducir, crear obras derivadas, mostrar y comunicar públicamente el contenido que comparten en la plataforma.

Meta recopila información personal de los usuarios, como nombre, correo electrónico, ubicación, intereses y comportamiento en la plataforma.

Meta utiliza esta información para mostrar publicidad personalizada a los usuarios.

Meta argumenta que la cesión de derechos es válida porque los usuarios la aceptan de forma voluntaria al descargar y usar sus aplicaciones.

No obstante, las políticas de privacidad son contratos de adhesión, lo que significa que los usuarios no tienen la posibilidad de negociar sus términos, esto genera una situación de desigualdad entre las partes, ya que Meta, al ser la empresa dominante, tiene el poder de imponer sus condiciones debido a que los usuarios no tienen control sobre cómo la empresa utiliza su contenido, incluso después de eliminarlo de la plataforma, por lo que Meta argumenta que su uso del contenido de los usuarios se ajusta a las excepciones de derechos de autor, como el uso para fines educativos o informativos.

Sin embargo, algunos expertos consideran que la interpretación que Meta hace de estas excepciones es demasiado amplia y podría estar violando los derechos de los usuarios.

ARGUMENTOS A FAVOR DE LA VULNERACION DE DERECHOS DE AUTOR.

Cesión amplia de derechos: La licencia otorgada a Meta es considerada por algunos como una cesión excesiva de derechos de autor,

Falta de control del usuario: Los usuarios no tienen control sobre cómo Meta utiliza su contenido, incluso después de eliminarlo de la plataforma.

Falta de transparencia: Las políticas de privacidad de Meta son extensas y complejas, lo que dificulta a los usuarios comprender el alcance de la cesión de derechos.

ARGUMENTOS EN CONTRA DE LA VULNERACION DE DERECHOS DE AUTOR.

Consentimiento del usuario: Al aceptar las políticas de privacidad, los usuarios consienten en la forma en que Meta utiliza su contenido.

Uso legítimo: Meta argumenta que su uso del contenido de los usuarios se ajusta a las excepciones de derechos de autor, como el uso para fines educativos o informativos.

Beneficios para los usuarios: Meta argumenta que la publicidad personalizada ofrece una mejor experiencia a los usuarios.

En los últimos años, ha habido algunos casos judiciales que han abordado la cuestión de la vulneración de derechos de autor en las políticas de privacidad de las redes sociales, como en el año 2020, un tribunal alemán dictaminó que Facebook no podía utilizar las fotos de los usuarios para publicidad sin su consentimiento expreso, aun así un tribunal de California dictaminó que las políticas de privacidad de Instagram eran válidas y no violaban los derechos de autor de los usuarios.

QUE PASA CON EL DERECHO DE IMAGEN EN LAS PLATAFORMAS DIGITALES.

En la era digital, las plataformas como Facebook, Instagram y TikTok han transformado la forma en que compartimos nuestra imagen personal, pues la cesión de derechos de imagen a estas plataformas genera interrogantes sobre la propiedad y el control sobre la propia imagen.

Cesión de derechos y propiedad de la imagen, al subir una foto o video a una plataforma digital, cedemos a la empresa una licencia para usar, reproducir, distribuir y modificar nuestra imagen, esta cesión de derechos puede ser amplia e incluso irrevocable, lo que significa que la empresa puede seguir utilizando nuestra imagen incluso después de que la eliminemos de la plataforma.

Consentimiento y contratos de adhesión, las plataformas digitales argumentan que la cesión de derechos de imagen es válida porque los usuarios la aceptan de forma voluntaria al crear una cuenta y subir contenido, no obstante, como en el caso de los derechos de autor, las políticas de privacidad y términos de servicio son contratos de adhesión, lo que limita la capacidad de los usuarios para negociar las condiciones.

Explotación comercial y control sobre la imagen, las plataformas digitales utilizan nuestra imagen para diversos fines, como publicidad personalizada, análisis de datos y entrenamiento

de algoritmos, esto genera preocupación sobre la explotación comercial de nuestra imagen sin recibir una compensación adecuada, además, la falta de control sobre cómo se utiliza nuestra imagen puede afectar nuestra reputación, privacidad e incluso seguridad.

MARCO LEGAL Y JURISPRUDENCIA.

El derecho de imagen está reconocido en la mayoría de las legislaciones del mundo, sin embargo, la aplicación de este derecho en el ámbito digital aún está en desarrollo. En algunos casos, los tribunales han reconocido que las plataformas digitales pueden ser responsables por la explotación comercial de la imagen de los usuarios sin su consentimiento.

RECOMENDACIONES Y FUTURO DEL DERECHO DE IMAGEN.

Es importante que los usuarios sean conscientes de los derechos que ceden al subir contenido a las plataformas digitales, por lo que se recomienda leer las políticas de privacidad y términos de servicio con atención, utilizar herramientas de privacidad para controlar la visibilidad de nuestro contenido y ser conscientes de los riesgos de compartir nuestra imagen en línea.

En el futuro, es probable que el debate sobre el derecho de imagen en el ámbito digital se intensifique, por lo que se hace necesario que se establezcan marcos legales claros que protejan los derechos de los usuarios y garanticen un uso responsable de su imagen personal.

Finalmente, la relación contractual entre las redes sociales y sus usuarios se caracteriza por una asimetría de poder, donde las plataformas ostentan una posición dominante. Esta situación exige mecanismos específicos para proteger a la parte débil: los usuarios. En este contexto, presentamos una propuesta que busca fortalecer la protección de sus datos personales y patrimoniales de derechos de la Propiedad Intelectual. Se busca establecer mecanismos para salvaguardar los intereses de los usuarios, promoviendo la transparencia mediante políticas claras y comprensibles, el empoderamiento del usuario a través de herramientas educativas y la gestión de datos personales, así como la mejora de la seguridad de datos y propiedad intelectual. Se propone establecer mecanismos de denuncia y resolución

de controversias, junto con la colaboración activa con organismos reguladores para asegurar el cumplimiento de normativas locales e internacionales. El proceso de implementación implica una auditoría de las políticas actuales, el desarrollo de recursos educativos, la actualización de términos y condiciones de manera accesible, una implementación gradual de cambios en la plataforma y un monitoreo continuo para evaluar la eficacia y realizar ajustes según sea necesario. En conjunto, esta propuesta busca equilibrar la relación contractual entre Meta y sus usuarios, fortaleciendo la confianza y contribuyendo al desarrollo sostenible de la comunidad digital en Meta.

REFERENCIAS.

Capítulo 1:

Leyes/Sentencias

Google LLC v. CNIL, Case C-507/17, 2019, ECLI:EU:C:2019:772, Court of Justice of the European Union.

Corte Constitucional de Colombia, Sentencia T-323/24, 5 de mayo de 2024, Sala Segunda de Revisión.

Comisión de Protección de Datos. (2023). Decisión sobre el cumplimiento de Meta con el GDPR en relación con la transferencia de datos (Caso Número: DPC-1001).

Agencia Española de Protección de Datos. (2022, 9 de junio). Expediente N.º PS/00222/2021.

Juzgado de lo Social N°. 2 de Alicante/Alacant. (2023, 15 de septiembre). Sentencia N° 190/2023, Recurso N° 489/2023.

Tribunal Europeo de Derechos Humanos, Tercera Sección. (2023, 4 de julio). Sentencia en el caso de la solicitud n.º 11519/20.

Audiencia Nacional. (2024, julio 4). Sentencia SAN 3693/2024 - ECLI:ES:AN:2024:3693.

Corte Constitucional de Colombia. (2023, agosto 3). Sentencia T-294 de 2023.

Artículos

Goodman, B., & Flaxman, S. (2017). "European Union regulations on algorithmic decision-making and a 'right to explanation'." AI Magazine, 38(3), 50-57.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). "The ethics of algorithms: Mapping the debate." Big Data & Society, 3(2), 1-21.

Zarsky, T. Z. (2016). "Incompatible: The GDPR in the Age of Big Data." Seton Hall Law Review, 47(4), 995-1020.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation." International Data Privacy Law, 7(2), 76-99.

Taddeo, M., & Floridi, L. (2018). "How AI can be a force for good." Science, 361(6404), 751-752.

Schwartz, P. M. (2019). Global data privacy: The EU way. New York University Law Review, 94(4), 771-861.

Bonet, L. (2021, julio 30). Amazon recibe la mayor multa de la historia de la Unión Europea en materia de privacidad: 746 millones de euros por no cumplir con el RGPD. *Xataka*. https://www.xataka.com/privacidad/amazon-recibe-mayor-multa-historia-union-europea-materia-privacidad-746-millones-euros-no-cumplir-rgpd

Libros

Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York: W.W. Norton & Company.

Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford: Oxford University Press.

Floridi, L. (2020). The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press.

Schwartz, P. M. (2022). Privacy Law Fundamentals (6th ed.). International Association of Privacy Professionals.

Reyes Trujillo, F. (2023). Vulneración de la privacidad de datos personales por empleo de la cámara de reconocimiento facial. Escuela Universitaria de Posgrado, Lima, Perú.

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Lizcano Luna, M. (2020). La inteligencia artificial como herramienta para la optimización del proceso judicial en Colombia.

Muñoz Torres, I. (2014). Aspectos legales y éticos de la seguridad informática.

Capítulo 2:

Leyes/Sentencias

Colombia. Congreso de la República. Código Civil, Ley 84 de 1873. http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html](http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html

Colombia. Congreso de la República. Ley 32 de 1886. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=100432](https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=100432

Corte Constitucional. Sentencia C-011 de 2013. Expediente D-9107. (M. P.: Alexei Julio Estrada

Corte Constitucional. Sentencia C-276 de 1996. Expediente D-1163. (M. P.: Julio Cesar Ortiz Gutiérrez

Corte Constitucional. Sentencia C-436 de 2013. Expediente D-9408. (M. P.: Mauricio Gonzales Cuervo; julio 10 de 2013.

Corte Constitucional. Sentencia T-367 de 2009. Expediente T-2141228. (M. P.: Jorge Iván Palacio Palacio.

Artículos

Eafit. (2024). Definiciones generales. Propiedad intelectual. [https://www.eafit.edu.co/institucional/propiedad-intelectual/Paginas/Definiciones.aspx](https://www.eafit.edu.co/institucional/propiedad-intelectual/Paginas/Definiciones.aspx

Herrera, M. (2010). Estado del derecho de autor o propiedad intelectual en la sociedad ecuatoriana. https://docplayer.es/62636395-Podium-revista-de-la-uees-no-18-samborondon-guayas-ecuador-enero-2010.html](https://docplayer.es/62636395-Podium-revista-de-la-uees-no-18-samborondon-guayas-ecuador-enero-2010.html)

Lizecita. (2023). Piratería en México. https://lizecita.wordpress.com/

Organización Mundial de la Propiedad Intelectual - OMPI. (2024). Crear valor a partir de la música los derechos que lo hacen posible. https://www.wipo.int/ip-outreach/es/ipday/2016/creating_value_from_music.html

Pérez, M. (2013). Gestión, tecnología e informática. https://es.slideshare.net/marisel2012/gestion-tecnologa-e-informtica2

Valencia, J. (2023). Música en la era de los algoritmos. Revista Razón Pública. https://razonpublica.com/musica-la-los-algoritmos/](https://razonpublica.com/musica-la-los-algoritmos/

Libros

Organización Mundial de la Propiedad Intelectual (OMPI). (2016). Principios básicos del derecho de autor y los derechos conexos. https://www.wipo.int/edocs/pubdocs/es/wipo_pub_909_2016.pdf

Organización Mundial de la Propiedad Intelectual (OMPI). (2023). La propiedad intelectual mejora la vida de las personas en todo el mundo. https://www.wipo.int/portal/es/](https://www.wipo.int/portal/es/

Pabón, J. (2009). Aproximación a la historia del derecho de autor: antecedentes normativos. Universidad Externado de Colombia.https://revistas.uexternado.edu.co/index.php/propin/article/view/457/3624

Capítulo 3:

Leyes / sentencias

Asamblea Nacional Constituyente. (20 de julio de 1991). Constitución Política de Colombia. Gaceta Constitucional 116 de 20 de julio de 1991. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Comisión del Acuerdo de Cartagena. (1993). Régimen sobre derechos de autor y derechos conexos. [Decisión Andina 351 de 1993]. Recuperado de: https://www.informatica-juridica.com/decision/decision-andina-351derechosautorconexos/#:~:text=Decisión%20Andina%20351%20de%2016%20de%20diciembre%20de,la%20Propuesta%20261%20de%20la%20Junta%3B%20Artículo%201.-

Comunidad Andina. (14 de septiembre de 2000). Régimen sobre la Propiedad Industrial. [Decisión 486 de 2000]. Recuperado de: https://www.cuc.edu.co/wp-content/uploads/2022/03/decision_486_de_2000.pdf

Congreso de Colombia. (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. [Ley 1581 de 2012]. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Corte Constitucional. (12 de septiembre de 2019). Sentencia SU-420 de 2019. M.P. José Fernando Reyes Cuartas. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm

Corte Constitucional. (8 de agosto de 2022). Sentencia T-280 de 2022. M.P. José Fernando Reyes Cuartas. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2022/T-280-22.htm

Corte Constitucional. (28 de septiembre de 2022). Sentencia T-339 de 2022. M.P. Jorge Enrique Ibáñez Najar. Recuperado de: https://www.corteconstitucional.gov.co/Relatoria/2022/T-339-22.htm

Corte Constitucional. (6 de julio de 2023). Sentencia T-241 de 2023. M.P. Natalia Ángel Cabo. Recuperado de: https://www.corteconstitucional.gov.co/Relatoria/2023/T-241-23.htm

Tribunal de Justicia de la Unión Europea. (4 de julio de 2023). Sentencia TJUE, Asunto C-252/21: Meta Platforms y otros. Condiciones generales del servicio de una red social. Recuperado de: https://cdeuv.es/documentos/menujuris/item/25605-sentencia-tjue-asunto-c-252-21-meta-platforms-y-otros-condiciones-generales-del-servicio-de-una-red-social-de-4-de-julio-de-2023.html

Artículos

Alvarado Carmona, M. (2017). Aspectos legales al utilizar las principales redes sociales en Colombia. Revista Logos, Ciencia & Tecnología, 8(2), 211-220. Recuperado de: https://www.redalyc.org/journal/5177/517752177019/html/

Burneo, B., & Antonio, J. (2008). Contratos de adhesión y mecanismos de protección al consumidor. Recuperado de: http://repositorio.uasb.edu.ec/handle/10644/497

Departamento jurídico de CEDRO. (3 de noviembre de 2022). Límites a los derechos de propiedad intelectual en las redes sociales. Recuperado de: https://www.cedro.org/limites-a-los-derechos-de-propiedad-intelectual-en-las-redes-sociales

Flórez, G. J., & Padilla, J. A. (2020). Los vicios de voluntad y la eficacia de los contratos de consumo. Universidad Externado de Colombia. Recuperado de: https://bdigital.uexternado.edu.co/handle/001/3480

Hawes, K. (2 de febrero de 2019). Legal Issues Using Electronic Contracts. Digital Age Lawyers. Recuperado de: https://www.digitalagelawyers.com/news/legal-issues-using-electronic-contracts

Keymer, D. S., & Troxler, S. V. (2008). Las cláusulas limitativas de la responsabilidad contractual en los contratos por adhesión. Recuperado de: http://repositorio.uchile.cl/tesis/uchile/2008/de-troncoso_d/pdfamont/de-troncoso_d.pdf

López, E. G. (2012). Cláusulas abusivas en los contratos de adhesión. Revista Chilena De Derecho Privado, 1(2), 139-173. Recuperado de: https://revistas.juridicas.unam.mx/index.php/derecho-privado/article/view/8983/11033

Rodríguez, R. R. (2004). Estudio comparativo de la formación de contratos electrónicos en el derecho estadounidense con referencia al derecho internacional y al derecho mexicano.

Revista Chilena De Derecho Privado, 1(9), 111-159. Recuperado de: https://revistas-colaboracion.juridicas.unam.mx/index.php/derecho-privado-ns/article/view/7170/6449

Libros y otros recursos

El Espectador. (19 de enero de 2023). Meta recibe multa de la UE por el mal manejo que les da a los datos personales. Agencia AFP. Recuperado de: https://www.elespectador.com/economia/meta-recibe-multa-de-la-ue-por-el-mal-manejo-que-le-da-a-los-datos-personales/

Meta. (2024). Nuestra historia. Recuperado de: https://about.meta.com/ltam/company-info/

Meta. (2024). Política de privacidad. ¿Qué es la política de privacidad y qué cubre? Recuperado de: https://www.facebook.com/privacy/policy/

Moreno Martínez, D. (2021). Responsabilidad Contractual de Facebook: contratos de adhesión atípicos y redes sociales. Semillero de Derecho Contractual Francesco Galgano, Universidad de los Andes. Recuperado de: https://semillerocontratos.uniandes.edu.co/responsabilidad-contractual-de-facebook-contratos-de-adhesion-atipicos-y-redes-sociales/

Legal Information Institute. (2021). Adhesion contract (contract of adhesion). Recuperado de: https://www.law.cornell.edu/wex/adhesion_contract_%28contract_of_adhesion%29

Legal Dictionary. (2014). Adhesion Contract - Definition, Examples, and Cases. Recuperado de: https://legaldictionary.net/adhesion-contract/

Juristopedia Editors. (2024). Contract of Adhesion: Legal Definition, Standard Form, Unfair Terms and Legal Protection. Juristopedia. Recuperado de: https://juristopedia.com

BBC News Mundo. (1 de febrero de 2024). Mark Zuckerberg se disculpa ante las familias de niños que han sufrido daños por culpa de las redes sociales. Recuperado de: https://www.bbc.com/mundo/articles/c72gze8r05jo

ANEXOS

Agencia Española de Protección de Datos	9 de junio de 2022
Expediente N.º: PS/00222/2021	

Juzgado de lo Social N°. 2 de Alicante/Alacant	15 de septiembre 2023

Sentencia 190/2023	Rec. 489/2023

TRIBUNAL EUROPEO DE DERECHOS HUMANOS	4 de julio de 2023
TERCERA SECCIÓN	Solicitud n.º 11519/20

Corte Constitucional de Colombia	2 de agosto se 2024
Sala Segundaa de Revisión	Sentencia T-323 de 2024

Tribunal de Justicia de la Unión Europea	24 de septiembre de 2019
Gran sala	Sentencia C-507 de 2017

Comisión de Datos se Irlanda (DPC)	22 de mayo 2023
DPC 1001	

Corte constitucional de Colombia	3 de agosto de 2023
Sala cuarta de revisión	Sentencia T-294 de 2023

Audiencia Nacional de Madrid	4 de julio de 2024
Sala de lo contencioso administrativo	Sentencia SAN 3693/2024 – ECLI:ES:AN:2024:3693